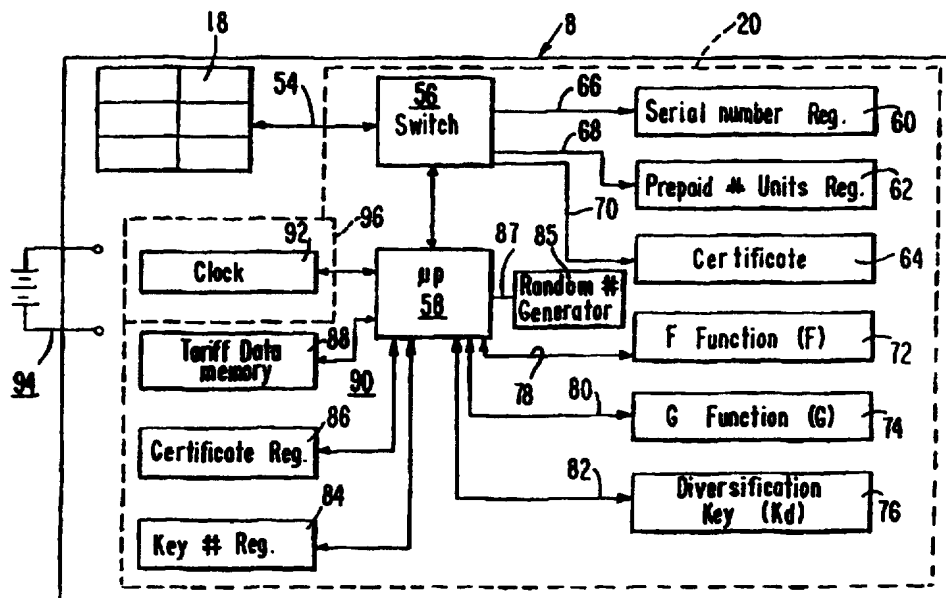




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04M 17/00, G07F 7/10		A1	(11) International Publication Number: WO 97/40616
			(43) International Publication Date: 30 October 1997 (30.10.97)
(21) International Application Number: PCT/IB97/00534		(81) Designated States: AU, BR, CA, JP, NZ, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 11 April 1997 (11.04.97)			
(30) Priority Data: 08/634,818 19 April 1996 (19.04.96) US 08/738,256 28 October 1996 (28.10.96) US		Published With international search report.	
(71) Applicant: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité de Gémenos, Boîte postale 100, F-13881 Gémenos Cédex (FR).			
(72) Inventors: MARTINEAU, Philippe; Suite 109, 6600 L.B.J. Freeway, Dallas, TX 75240 (US). LAMB, George; 3024 Country Squire Lane, Decatur, GA 30333 (US).			
(74) Agent: NONNENMACHER, Bernard; Gemplus S.C.A., Voie Antiope, Zone Industrielle Athélia III, F-13705 La Ciotat (FR).			

(54) Title: PREPAYMENT FOR WIRELESS TELEPHONE SERVICES BY MEANS OF SMART CARDS



(57) Abstract

It's a prepaid smart card to be used in a wireless telephone network and method for prepaying for wireless telephone services, and a system for operating a wireless telephone network with prepaid smart cards. The cards, method and system permit the use of wireless telephones anonymously, and/or the payment by a user without having a subscription. The invention requires minimal changes to the existing wireless telephone and wireless telephone network, yet provides security against abuse or fraudulent use of the system. Additionally, promotional material may be provided with the prepayment or persons may prepay into a subscriber's telephone.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TITLE OF THE INVENTION

PREPAYMENT FOR WIRELESS TELEPHONE SERVICES BY MEANS OF SMART CARDS

5

TECHNICAL FIELD

The invention relates generally to prepaid smart cards for the delivery of goods/services, and to the use of such prepaid smart cards with subscriber identity modules, and which for
10 example may find particular application in cellular or wireless telephone networks.

BACKGROUND ART

The invention is a method and apparatus and will be
15 described with particular application to a cellular or wireless telephone and network of the GSM type. It should be understood however that the invention is not limited to such GSM cellular wireless network nor to telephones, but may find application elsewhere, and wherever there is the provision of services
20 and/or goods which are paid for with prepaid smart cards.

Integrated circuit cards are smart cards, or electronic chip cards, which are usually the size of a conventional credit card, with six or eight small electrical contacts on one face, and contain an integrated circuit with a memory and may include
25 a microprocessor. The newer type of cards are of the "contactless" type, i.e. the contacts are not electromechanical and there is no physical contact. There is a small loop or antenna inside the card, which makes electromagnetic or induction contact with a card reader terminal and with the
30 integrated circuit in the card. This type of card is shown for example in U.S. Patents 4,874,934 and 5,206,495 presently owned by the same assignee as in this application. When the term

-2-

"contacts" is used here and in the claims of this patent application, it should be understood that it includes both the electromechanical and electromagnetic contacts. IC cards which include a microprocessor are sometimes called smart cards.

5 Data and programs for manipulating data and communicating outside the card are included in the integrated circuit. In the past, prepaid cards have been widely used in the purchase of telephone services, particularly in France and Germany, where public pay phones accept the cards instead of coins.

10 Typically, the cards are purchased at the post office for a specified amount. The cards are inserted in a public pay telephone. Connection is made and units of value are removed or subtracted from the card during the telephone call. The mechanical and electrical specifications of the cards are
15 standardized, and one set of standards is published by ANSI, American National Standards Institute, 11 East 42nd Street, New York, NY 10036 under the title "Identification cards-Integrated circuits cards with contacts" ISO 7816-1 and ISO 7816-2. Such cards are manufactured by and are commercially available from
20 several companies, including applicant's assignee, Gemplus Card International, avenue du Pic de Bertagne, Parc d'Activités de la Plaine de Jouques, 13420, Gemenos, France.

Cellular wire networks are widely spread across the globe today. These networks are built to one of a few technical
25 standards, which are GSM, DCS 1800, and PCS 1900. The present invention is described with reference to GSM but is not limited to GSM. The standards on wireless networks may be obtained from ANSI. Particular attention is directed to standard ETSI/GSM 11.11. Those wishing additional information on
30 cellular wireless telephone and operation are referred to a number of books in the field, for example Mouly, Michel and Pautet, Marie-Bernadette, The GSM System of Mobile

-3-

Communications, 1993, Loissoy-les-Chateaux, France, Europe Media Duplication S.A.; or Clayton, Michael, GSM Global System for Mobile Communications (19__), North Sidney, Australia, Security Domain Pty Limited.

5 These cellular technologies use the latest techniques. The more modern cellular wireless networks use a subscriber identity module, SIM, which is on a smart card which is inserted into the wireless handset. The SIM identifies the subscription to the cellular wireless network. Earlier model
10 cellular telephones had the SIM permanently installed in the handset, but in modern equipment it is in a removable smart card. The advantage of a removable SIM is that a subscriber may carry his SIM with him, and insert it in any cellular telephone which will accept the card. This permits him both to
15 use the card and to be billed on either his home number, or his account.

 To use a cellular telephone, one needs a SIM. It is estimated that 40% to 50% of telephone users do not have sufficient credit to obtain issuance of a SIM. Several schemes
20 have been proposed for permitting prepayment of calls from wireless terminals where the user would insert a prepaid card similar to the prepaid cards used in public telephones in France and Germany. One such application is described in the parent application, Serial No. 08/634,818, filed on April 19,
25 1996. Alternative approaches are provided for in the GSM standard, but have proved to be cumbersome. An aspect of the present invention is to permit prepayment of telephone calls from a cellular wireless telephone handset so that the call is not charged on the account of the registered SIM holder. It
30 should be noted here that in the GSM system, the subscriber number, which is called an International Mobile Subscriber Identity, IMSI, is attached to an individual. In the GSM based

-4-

network, the IMSI number is stored in the SIM card. When inserted in the handset, the SIM provides information about the subscriber to the network that is necessary for establishing the call and for billing the call.

5 Because of this existing arrangement of providing cellular wireless service, there is lost those potential customers who cannot qualify as subscribers and who thus do not get any service. If we base this on today's analog subscription rate, then 40%-50% of people applying for subscription have been
10 denied credit and denied service.

 Depending on the country and also depending on the distribution method in that country, the problem can get more serious. In Europe, for example, the subscription process occurs at the point of sale. If the credit check at the point
15 of sale proves to be negative, then the user will be refused service without having to purchase any goods. However, in North America an individual can buy a "ready to go" package in many different consumer stores, such as Radio Shack, Wal Mart without having to sign any contract at the time of purchase.
20 The subscription process is done over-the-air later, usually at home. Consequently, the potential user can spend a few hundred, e.g. \$200, for a package that he is not guaranteed to get any service from. And, this is a major problem that has not been solved to date.

25 In the prepaid card envisioned by the present invention, the billing of the call would not be to the identified subscriber, as in the IMSI and SIM, but would be paid from the credits in the prepaid card.

 The apparatus, method and system of the present invention
30 might also permit anonymous use, i.e. a party could have a SIM card that did not identify a particular individual or

-5-

subscriber. It would be an anonymous SIM, with payment by prepaid card.

In another application, a person wishing to use another person's cellular telephone, but not have the call billed to that person, could use the prepaid card and pay for the cellular call as used. Alternatively, one could give a present to a cellular user by storing prepaid units in the wireless telephone.

There have been several attempts to provide a prepaid type of service over GSM. But none of them truly provides the solution expected by network operators. One solution is to monitor use from the network, and to bill a prepaid card in the handset in real time. A second solution proposed is to use a service sometimes called Advice of Charge, AOC, which is more fully defined by GSM 11.11. Both of these solutions have drawbacks.

The first solution, prepayment managed from the network, is a viable alternative but with shortcomings. It is very expensive for the network operator. It requires an intelligent networking infrastructure, INI, with Hot Billing, HB, capability as well as a network capable of on-line tax or rate information. The user remains attached to a SIM card and is managed as a subscriber.

The second solution AOC provided by GSM was not intended for prepayment type of applications but more for family usage or rental applications. In AOC, there was always a subscription attached to the account. The "prepaid mode" was not reflected in the final bill. The subscriber can at any time turn his subscription into a restricted mode when he wants to lend his handset to someone. In this mode, the units are decremented in the card using a network-base telephone schedule of charges until all units have been consumed. Although it can

-6-

be assimilated to prepaid applications, it is charged on the subscriber's bill, and he remains responsible for the calls. Also, such implementation suffers from a lack of security. It is not intended for prepaid applications. And it is believed to be subject to probable fraud.

The previous GSM systems require identification of at least the purchaser of the cellular telephone, and there is no such thing as an anonymous user of a cellular telephone.

DISCLOSURE OF THE INVENTION

There is definitely a need to address the market segment of the "credit challenged" individuals in a different way than GSM can provide today. There have been several attempts to provide a "prepaid type" of service over GSM. But, each one does not truly provide the solution expected by network operators. A first solution is to monitor units from the network, and to bill a prepaid card in the handset in real time. A second solution proposed is to use a service sometimes called "Advice of Charge", AOC, which is more fully defined by GSM 11.11. Both of these solutions have drawbacks. The first solution, prepayment managed from the network, is a viable alternative, but with shortcomings. It is very expensive for the network operator. It requires an Intelligent Networking infrastructure, IN, with Hot Billing, HB, capability, as well as a network capable of on-line tax or rate information. In this prepaid managed system, the user remains attached to a SIM card, and has still to be considered as a subscriber and has to be managed as such.

The second solution, AOC, provided by GSM was not intended for prepayment type of applications, but more for family usage or rental applications. In AOC, there is always a subscription attached to the account. The "prepaid mode" is not seen from

-7-

the billing, and is not reflected on the final bill. The subscriber can at any time turn his subscription into a restricted mode when he wants to lend his handset to someone. In this mode, the units are decremented in the card using network based telephone schedule of charges until all units have been consumed. Although it can be assimilated to prepaid applications, it is never reflected on the subscriber's bill who remains overall a "credit worthy subscriber". Also, such implementation suffers from a lack of security, and is not intended for prepaid applications initially, and is believed to be subject to probable fraud.

All of the previous GSM systems require the user (or at least the purchaser of a cellular phone) to be identified. There is not such thing as an anonymous user of a cellular telephone. An object of the present invention is to provide a cellular telephone which may be used completely anonymously.

A further object of the invention is to provide a prepaid telephone service, which has enhanced security or put another way reduced opportunity for fraudulent use.

An object of the invention is to provide an apparatus and method and smart card, which will provide a network independent prepaid service based on a fixed tariff structure that will be offered to "credit challenged" individuals in the form of a prepaid throw away smart card.

In an alternative embodiment, the smart card may be used continuously in that new prepayment value may be placed in the card. As of today, GSM defines a "Mobile Station", MS, as having a "Mobile Equipment", ME, and a "Subscriber Identify Module", SIM; $MS = ME + SIM$. Such a combination is mandatory for operating a service. According to an aspect of the invention, the SIM is no longer attached to a subscriber, but will be identified to the network operator as an anonymous

-8-

prepaid type SIM. Prior to sale of the telephone, such a SIM would be programmed and inserted into the handset. It would be a SIM with restricted capabilities, e.g. 611 calls allowed only. If the purchaser wished to convert his SIM to a traditional subscription of a cellular phone, he could initiate the subscription process, OTA, and the SIM could be turned into a full subscription attached to a user after approval of the user's credit check. In the case of the credit check being unsuccessful, or if the user wished, there would be another card in the package with the cellular telephone with an amount of units already loaded, to be inserted in an additional slot reserved for that purpose in the handset.

Because of that additional card, the user could still benefit from a wireless service without passing the credit check by using the additional card. Once the card was consumed, i.e. all of the units or value of the card had been used in calls, the user could buy another card to continue with the service. This provides the network operator with a secure financial position for such individuals, provides the user of cellular service who may wish to remain anonymous, the ability to do so. Also, for the user who has good credit and who wishes to retain traditional service, and for the user who is credit challenged, as well of the vendor of cellular equipment to users, a one-stop shopping solution.

The concept and implementation as proposed herein opens the door to an untouched area of promotional campaign wherein a third-party could offer cellular air time by mailing prepaid cards as part of the marketing program. It turns the handset into a cellular prepaid phone.

An object of the invention is to provide cards, methods, apparatus and systems for prepaid cards for use with a GSM or other network that is easy to use, addresses issues of

-9-

security, and is thrifty for both the user and the network operator.

Another object is to provide an easy-to-use secure prepaid wireless communication system which integrates existing standards, and provides a minimum of new standards and new structure into the existing GSM network.

According to an aspect of the invention, there is provided a method for enabling service from a wireless telephone having a SIM and a prepaid card in the telephone comprising the steps of calculating in the card a certificate as a function of (i) number of prepaid units remaining in the card, (ii) serial number in the card, and (iii) a key number in the card; and transferring from the card to the SIM (i) said number of prepaid units remaining in the card, and (ii) the card's serial number; then calculating in the SIM a number which should be the same as the card key number based on said transferred number of prepaid units remaining in the card and said card serial number; and calculating in the SIM a certificate as a function of said transferred number of prepaid units remaining in the card and said calculated number which should be the same as said key number in the card; then comparing said calculated certificates from said card and from said SIM; and then if coincident in said comparison then enabling said telephone in said network.

According to a further aspect of the invention there is provided an apparatus which automatically performs the steps of the first described method.

According to another aspect of the invention, there is provided a modified prepaid secure smart card which in normal use in a network allows the transfer of goods/services to a user of the card from a network operator by subtracting prepaid units of value stored in said card in exchange for said

-10-

goods/services. The card is a card-shaped carrier having a terminal, and an integrated circuit embedded in the carrier and connected to said terminal. The integrated circuit includes a serial number register for storing a serial number unique to each card; a prepaid units register for storing a number of units of prepaid value; a switch responsive to interrogation at the terminal to write to the terminal the serial number in the serial number register, and to write to the terminal the number of prepaid units remaining in said units register; a key number register storing a key number, which has a first portion unique for each card, and a second portion which is common to a plurality of cards, and which is unique for a network operator, the key number in normal use of said card is not readable at the terminal; an algorithm stored in said card, said algorithm in normal use of said card not being readable in said terminal, and a microprocessor for calculating a certificate in accordance with the algorithm as a function of the key number and the number in the prepaid register, and the certificate being readable at the terminal.

According to another aspect of the invention, there is provided an improved subscriber identification module, SIM, for operating with prepaid cards and with a network that provides goods/services via said network. The SIM includes an integrated circuit having, an input for receiving from one prepaid card (i) a serial number of said card, (ii) a number of prepaid units remaining in the card, and (iii) a certificate compiled by said card from its serial number, card key number, an algorithm therein, and number of prepaid units remaining in the card; a diversification key which is the same for a plurality of modules of a network; first and second algorithms; a microprocessor for calculating (i) a card key number with the first algorithm as a function of the diversification key, and

-11-

the receive serial number of the card, and where the calculated card key number should be the same as the key number in said card; and (ii) calculating a certificate with the second algorithm as a function of the calculated card key number, and the receive number of prepaid units remaining in the card; and (iii) comparing the calculated certificate with said received certificate, and (iv) if coincidence, generating an enable signal whereby goods/services are provided in accordance with said generated enable signal.

According to a further object of the invention, there are provided integrated circuits of the types first described in the preceding two paragraphs for use in prepaid smart cards, and for use in SIMs.

According to an aspect of the invention, there is provided a method of prepaid cellular telephone calling with a prepaid card which has the steps of validating a number of prepaid units of a prepaid card; recording the number of validated prepaid units in a SIM in a cellular telephone, and also recording the number of validated prepaid units at a network operator; calculating the number of prepaid units as a call progresses at two separate locations with the calculations being done independently, one being associated with the SIM and the other in the network operator, and interrupting a call-in-progress, when either of the calculations shows no remaining prepaid units.

In a further aspect of the invention, the validation determining if the prepaid card is for service with the network operator; transmitting from the prepaid card to the network operator a number of units to be validated from the card and a certificate number of that card; and comparing in the network operator the certificate number and the number of units transmitted from the card, with a certificate number and a

-12-

number of units for the cards independently received by the network operator. In another aspect, the recording step includes having a first meter in the SIM and a first meter in the network operator, both of the first meters being set; and
5 setting a second meter in the SIM and second meter in the network operator to a number of units different from the number of units in the first meters each by an amount corresponding to the number of validated prepaid units. Additionally, in
10 another aspect of the invention, the calculating includes increasing the number of units in both the first meters in accordance with air time usage of the telephone; and comparing the number of units in the first and second meters in the SIM and comparing the number of units in the first and second meters at the network operator.

15 Another part of the invention is an addition to a wireless telephone network which has equipment for operating a wireless telephone network of wireless telephones according to a protocol. A card data base is added having information on a plurality of prepaid cards which are to be used in wireless
20 telephones on the network. The data base includes for each card to be used in the network (i) a serial number of the card, (ii) a number corresponding to units of prepaid telephone calls, (iii) a certificate number which is a function of the card's serial number and the number of units. A supervisory
25 control module validates each card when first used on the network by comparing the card's certificate number as received from a wireless telephone having the prepaid card therein, with the corresponding numbers for the card stored on the card data base. Apparatus downloads a message from the prepaid card to
30 the wireless telephone that units are transferred from the card to the telephone; and sends a signal to the data base that the number of units associated with the card number has been used.

-13-

Another aspect of the invention is a mobile telephone handset with telephone circuitry to communicate with a wireless network operator in accordance with a protocol. A slot receives a removable SIM card; and the slot also accepts a removable prepaid card. The card has (i) a serial number, (ii) a number corresponding to units of prepaid telephone time, (iii) a number corresponding to the network in which the card may be used, and (iv) a certificate number which is a function of the serial number and the number of units. The SIM card includes a storage whose contents correspond to prepaid units remaining available to be used for calls, and a flag when set indicating if a telephone call is to be paid with the prepaid units.

The invention also envisions a data disk for use in a mobile telephone network, which provides for prepaid cards on the network and in which a number corresponding to value of prepaid calls is stored on cards and transferred to telephone handsets operable on the network. The data disk has identification numbers of each card with prepaid value which may be used on the network, an identification number of the network in which the cards are to be used, a number representing the value of prepaid calls stored on each card, and a signature of each card, the signature being a function of the card's identification number and number of units. The data disk is readable at the network operator and the data thereon is storable at the network operator for use in accepting and keeping records of the prepayments and calls placed against the prepayment. The disk may also have in the signatures a function of the network operator identification number.

An aspect of the present invention is a pre-paid chip card for use in a mobile telephone handset in a mobile telephone network. The card has an integrated circuit with a memory and

-14-

stored therein (i) a first number representing a serial number of the card; (ii) a second number representing value of prepaid telephone calls to be made from a mobile telephone; (iii) a third number representing a mobile telephone network in which the card may be used; (iv) a fourth number representing a certificate, which is a function of the first and second numbers; (v) a message string which is to be displayed on a mobile handset. The card includes circuitry operable in response to signals from the handset for enabling the numbers from the memory to the handset when the card is inserted into the mobile telephone handset, and for enabling the message string to be displayed on the handset. Also, the card may include in the signature a function of the third number.

The invention is also a method of operating a mobile telephone system with prepayment in which the system has a network operator, a plurality of handsets each with a removable SIM card, a plurality of prepaid cards each with prepaid units, and a certificate. The method includes the steps of removing the SIM card from the handset and replacing the SIM card with a prepaid card; entering from the prepaid card into the handset, (i) a number of prepaid units and (ii) the certificate number; transmitting from the handset to the network operator the number of prepaid units entered from the card and the certificate number entered from the card, verifying at the network operator the validity of the number of units and the certificate received from the handset, and if correct, then transmitting to the handset a message for increasing an accumulated call meter max in the SIM card by the number by the number of units as verified by the network operator.

When a call is made, the method debits an accumulated call meter, ACM in the SIM card for each unit of air time, compares the ACM with the ACM MAX, and permits the call to continue as

-15-

long as the ACM is less than ACM MAX, and signaling the network operator for interrupting the call when the ACM value is at ACM MAX. Whereby a call continues as long as credit remains between ACM and ACM MAX.

5 These other features of the invention become more apparent from the preferred embodiments described with reference to the attached drawings, which are for purposes of illustration and do not limit the invention.

10 These and other objects and features of the invention will become more apparent from the preferred embodiments described with reference to the attached drawings, which are for the purposes of illustration and not limiting of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

15 Fig. 1 is a schematic drawing showing a cellular telephone handset and cards of the invention, and a network operator's base station.

20 Fig. 2 is a schematic block diagram showing various elements in a prepaid smart card and in an integrated circuit in said prepaid smart card.

 Fig. 3 is a schematic block drawing illustrating various elements in a SIM in a cellular telephone handset.

25 Fig. 4 is a schematic drawing showing an alternative embodiment of a cellular telephone telephone handset and cards and a network operator.

 Fig. 5 is a schematic block diagram showing a prepaid card an various elements in an integrated circuit in the prepaid card in the embodiment of Fig. 4.

30 Fig. 6 is a schematic block drawing illustrating various elements in a SIM of the embodiment of Fig. 4.

 Fig. 7 is a schematic diagram of a portion of the network operator's station of the embodiment of Fig. 4.

-16-

Fig. 8 is a flow chart illustrating validation of a prepaid card in a cellular telephone handset and entry of a number of prepaid units in the SIM and in the supervisory control module of Fig. 7 of Figs. 4-7.

5 Fig. 9 is a flow chart showing the call approval routine for calls from a cellular telephone which has validated prepaid units stored in the SIM card and registered in the network operator's supervisory control module of Fig. 4-8.

10 Fig. 10 is a schematic drawing of a prepaid card showing another alternative embodiment of a prepaid card in which some, but not all of the prepaid units may be transferred from the prepaid card to the SIM and the network operator's supervisory control module.

BEST MODES FOR CARRYING OUT THE INVENTION

15 Fig. 1 shows a cellular telephone handset 2 having two slots therein 4 and 6. The slot 4 is to receive a removable SIM mounted on a miniaturized smart card 8. The slot 6 is to receive a prepaid card 10 which is shown here on a conventional smart card 10, which is to the ISO standard cited above. In
20 operation, the cellular phone 2 communicates through its antenna 11 with a cellular telephone operator's base station 12.

Fig. 2 is a highly schematic portrayal of the prepaid card 10. The card has six or eight contacts 14 on one face and an
25 electronic circuit embedded in the card which in current manufacturer would be a single integrated circuit 16. The integrated circuit is embedded in the card usually below the contacts 14. According to the ISO standard, the card is 85 millimeters long, 54 millimeters wide, and 1 millimeter thick.
30 The contacts 14 are six or eight in number, and occupy an overall area of not more than 9.62 mm x 9.32 mm. Each contact typically is not less than 1.7 x 2 mm. The contact area begins

-17-

typically 10.25 mm from the left edge and 9 mm from the upper edge of the card. The integrated circuit 16 typically is 1 or 2 mm on each side a fraction of a mm thick when mounted on a support. Thus it would be appreciated that the drawing of Fig. 2 is highly schematic.

Fig. 3 is a schematic view of a SIM card 8 as shown in the drawings here as the small physical version smart card with the typical dimensions of 25 x 15 x 1 millimeters; with the contact area substantially the same as in the large card. It would be thus appreciated that the drawing of Fig. 3 is highly schematic in its showing of the card 8 with contacts 18 and an integrated circuit 20.

Alternatively, the SIM may be mounted on a full size smart card or may be non-removably mounted in the handset. The slots 4 and 6 have the necessary connectors with contacts for making electrical connection to the contacts 14 and 18 on the cards 8 and 10.

Before describing in detail the Figs. 2 and 3, let us look at some of the overall operations and structure.

First, no modification to the existing GSM air interface between the handset 2 and the base station 12 is required.

Tax or telephone charge information is computed by the handset during the call. This may be based on a "unit value table", UVT, stored in the SIM. The tax information may be computed on the basis of a flat rate (e.g. using an internal clock of the handset), and for that reason in one embodiment, it will not allow roaming of the networks. Alternatively, the tax information may be provided by the network in which case roaming may be permitted. The table in the SIM is updated "Over the Air", OTA, at any time, once the handset has established connection with the network. The OTA update

-18-

capability offers flexibility in the management of the unit pricing.

The SIM plays the role of a security module that will secure the exchange with the prepaid card. The handset manages the exchange between the two cards and offers full telephone service only if a prepaid card with units left in it is inserted and has been authenticated; or if the "initially restricted" SIM has previously been turned into a "full subscription" SIM or otherwise it will offer restricted service, 611. It is believed that the handset is initially packaged and sold with a initially restricted subscription SIM and a prepaid card. The plug-in SIM is initially restricted. It has a subscription in "fixed dialing number", FDN, mode allowing calls to 611 only. The plug-in SIM is plugged into the handset. The prepaid card is loaded with units representing a value. For example, \$10, which for example, represents 50 units of \$0.20 each.

The prepaid card 10 has information, which is readable outside of the prepaid card, namely, the number of units remaining in the card, and a serial number of the card. Invisible in the card, i.e. which cannot be taken out of the card is a function or algorithm, F, and a key for that algorithm, Kn. The algorithm and the key are used by the prepaid card for making certain calculations.

The organization and data flow in one embodiment will now be described and we will need to form on two separate steps. First, an initial session set-up; and then, the decrementation process during a call.

The SIM in the cellular telephone is already active in the network when purchased. However, it is configured in "FDN" with all calls routed to the Customer Care Service center, CCS. If credit is sought and approved, the SIM is updated Over the

-19-

Air, OTA, and the FDN restriction is turned off. If not, the SIM remains in the restricted mode and no calls can be placed other than to customer service or as programmed in the FDN list. At that point, the prepaid card needs to be inserted to get service.

A typical initial session set-up would be as follows.

Before allowing any calls, the prepaid card in the handset needs to be authenticated to validate that it is a card really issued by the "Network Operator", NO. This is achieved by matching a "certificate" associated to the number of units claimed by the prepaid card. The SIM and the prepaid card are both inserted in the handset. The SIM is initially programmed with a function F that is the same as the function F in the prepaid card. To verify the certificate, the SIM recomputes the key number Kn. This is done using a diversification key Kd and another secret function G.

$$Kn = G (Ser.nb, Kd)$$

In the prepaid card, the certificate is computed by the prepaid card from the number of units left, Xunits, using a formula involving the secret function or algorithm F, which is the same as the function F in the SIM, and a secret key Kn, which is stored in the prepaid card:

$$Cert = F (Xunits, Kn).$$

The secret key Kn in the prepaid card is unique for each individual prepaid card.

The handset or SIM causes certain data to be read from the prepaid card to the SIM, namely Xunits, Ser.nb, and Cert1.

The SIM then computes

$$Kn = G (Ser.nb, Kd)$$

and using that calculated Kn, then calculates

$$Cert = F (Xunits, Kn)$$

-20-

A comparison is made, and if $Cert = Cert1$, then the prepaid card is authenticated. If the prepaid card authentication fails, the SIM stays in the FDN mode, and calls remain restricted to the FDN list. If the authentication is
5 successful, the SIM automatically turns off the FDN mode or to a non-restricted mode to offer full network access either for outgoing or for incoming calls.

During the initialization of the call, it is prudent for the SIM to generate a random number to the prepaid card. The
10 certificate generated in the prepaid card is a function that includes the random number, Rdn , i.e.:

$$Cert = F(Xunits, Kn, Rdn)$$

Similarly, in the SIM, the calculation of the certificate also includes that random number so that the SIM after computing Kn ,
15 then calculates

$$Cert = F(Xunits, Kn, Rdn)$$

This avoids the possibility of tampering with the first unit with a prepaid card.

An alternative approach might be to not include the random
20 number in the first calculation, i.e. in the initialization, but to make the first time period until the prepaid card is decremented very short, i.e. a second or two, and then after that initial short time, to decrement the prepaid card one unit, the decrementation of the card being performed with a
25 random number.

The decrementing of prepaid units during calls involves an exchange between the SIM and prepaid card. Every time a call is placed, the handset starts measuring time using its internal clock, and uses a table stored in the SIM to convert an amount
30 of time into a number of units to decrement. Then, when units have been "decremented in the prepaid card", the process is as follows.

-21-

The handset has a SIM with F, Kd, G, random number generator.

The prepaid card in the handset has, Xunits, Ser.nb, F, and Kn.

5 The handset causes the number of prepaid units remaining in the prepaid card to be passed to the SIM, i.e. Xunits is read into the SIM. The handset asks the SIM to generate a random number Rdn. The SIM generates the random number, Rdn, as a parameter to ensure security, and to avoid someone trying to replay the same sequence. The random number is sent from
10 the SIM to the prepaid card, and a pulse or other signal is sent to the prepaid card to decrement at least one unit, for example n units. In the prepaid card, n units are decremented, so that

15 $X_{\text{left}} = X_{\text{units}} - n.$

The prepaid card then computes a new certificate, or result, which is based upon the function F

$$\text{Result} = F (X_{\text{left}}, \text{Rdn}, \text{Kn})$$

This is a new certificate, except that the Result includes as a
20 variable the random number just received. The handset then sends back to the SIM the Result and the remaining number of units in the card. The SIM then recomputes the Result to verify that the units have been decremented:

$$\text{Result} = F ((X_{\text{unit}} - n), \text{Rdn}, \text{Kn})$$

25 The Kn, it should be noted, at the SIM is previously computed from the formula $\text{Kn} = G (\text{Ser.nb}, \text{Kd}).$

 If the result computed by the SIM matches the one from the prepaid card, it verifies that units have really been decremented. Thus, the SIM continues to operate normally. If
30 the results as calculated in the SIM, and as received from the prepayment card are different, then the SIM turns back to the FDN mode and restricts the cellular phone to the FDN list.

-22-

This decrement process continues during the call until either the call is terminated, or there are no more units left in the prepaid card.

At the end of each session, when the handset is turned
5 off, the temporary "non-restricted" mode disappears; and at the next session "power on", the SIM will automatically start in the FDN mode. In other words, the telephone is in the restricted or FDN mode when power is first turned on. If the SIM and prepaid card authenticate that there are units in the
10 prepaid card in the initialization of a step, the SIM switches to a non-restricted mode. The telephone remains in the non-restricted mode until there are no more units remaining in the prepaid card, which would usually be due to the certification not matching as each unit is decreased, or if the telephone is
15 powered off and then is powered on.

Some characteristics of the different elements may be noted.

The number of units remaining Xunits in the prepaid card is a variable.

20 The serial number, Ser.nb, in the card is a fixed number. It is unique to each card. Typically, it is 20 characters in length. The function F in both the prepaid card and the SIM are the same function. It is a coding algorithm and for example of the DES type. DES is a commonly used sophisticated
25 algorithm developed by the U.S. National Bureau of Standards for encrypting and decrypting data. There is the encryptions standard DES, which uses a key. This or any type of convenient or conventional encryption system may be used.

The key number Kn is a fixed number in the prepaid card,
30 and is the key to the function F. It is unique to each card and includes within it at least one character which identifies

-23-

each network operator. This permits cards of one network operator to be used only in its network.

In the SIM, the secret function G is a fixed algorithm and as the F secret function may be DSQ or any other convenient or conventional type. The diversification key Kd for the secret function G, is the same for all SIMs of that network operator, typically, 16 characters. The Kn is calculated by the SIM from G (Ser.nb, Kd).

Turning now to Fig. 2, there is shown the contacts 14 connected by a bus 24 to the integrated circuit 16. The bus 24 comes into a switch 26 which is operated by a microprocessor 28. The serial number of the card or integrated circuit is stored in serial number register 30. The number of units remaining in the card is stored in a prepaid number of units remaining register 32. The serial number register and prepaid number of units remaining register are shown connected by buses 34 and 36 to the switch 26. This is to indicate that the serial number and number of units remaining may be interrogated from outside the card through the contacts 14. Importantly, the actual arrangement of the switch, microprocessor, and the registers as now described may all be in a single portion of the microprocessor depending upon circuit design.

The algorithm or function F is stored in a function register 35, and the key number Kn is stored in a key number register 37. As shown in the drawing, these are connected by buses 38 and 40, respectively, to the microprocessor 28, which in turn is connected to the switch 26. The purpose here is to ensure that the function F and key number Kn are invisible at the contacts 14 and cannot in normal use and operation of the prepaid card be read out at the contacts 14.

The certificate is calculated in the microprocessor 28 and may be stored in a certificate register 42. The certificate is

-24-

passed to the contacts 14 in reply to an interrogation, and under control of the switch and microprocessor.

The random number Rdn received from the SIM, may be stored in a random number register 46 shown connected to the microprocessor by bus 48. The recalculated certificate with the random number may be stored in the certificate register 42, and is transferred as needed to the contacts 14.

With regard to the various elements shown in Fig. 2 as being on the integrated circuit, it will be appreciated that the switch, microprocessor, and several registers may be all contained within a single chip. Also the element may not be allocated to unique space within the IC memory, for example, the various numbers in the registers may be moved around under the control of the microprocessor. This would be in accordance with the design of the particular IC chip.

The important point is that the serial number, number of prepaid units remaining, and certificate can be read from outside the prepaid card through the contacts 14. The function F and the key number Kn can normally not be interrogated from the contacts 14. Supervisory controls, not shown, may be included in the integrated circuit to permit such an interrogation based upon a higher level of security than what is shown.

The serial number, function, and key number may be written into the integrated circuit at time of manufacture, or subsequent to manufacture. Any convenient or conventional type of circuit and method for the entry of such data may be used.

Turning now to Fig. 3, there is shown the SIM arranged on smart card 8 with the contacts 18 and an integrated circuit 20.

The contacts 18 are connected by a bus 54 to the a switch 56 and the switch is connected to a microprocessor 58.

-25-

A serial number register 60, a prepaid number of units remaining register 62, and a certificate register 64, are connected to a switch 56 by buses 66, 68 and 70, respectively, and receive and store the serial number, remaining number of prepaid units, and certificate number as received from the prepaid card through the contacts 18 and the switch 56, and under the control of a microprocessor 58. The switch 56 and the microprocessor 58 may be one and the same unit, although the microprocessor controls the switching function.

The function or algorithm F is stored in a F function register 72; the G function or algorithm is stored in a G function register 74; and the diversification key Kd is stored in a diversification key register 76. These three registers are shown connected by buses 78, 80 and 82, respectively to the microprocessor only because they cannot normally be read out from the SIM at the contacts 18. The key number Kn is computed by the SIM as a function of the G function operating on the serial number and the diversification key, and the key number is stored in a key number register 84. A random number generator 85, generates a random number, Rnd on a bus 87 connected to microprocessor 58. The microprocessor then calculates a certificate from the key number stored in the register 84, the F function stored in the F function register 72, the serial number in register 60; and number of units remaining in register 62. The calculated certificate is then stored in a register 86.

Comparison between the certificate calculated by the SIM in register 86 and the certificate received from the prepaid card in register 64 is performed in the microprocessor 58. Alternatively, it could be performed in a separate counter (not shown).

-26-

Tariff data as received from the network operator is stored in a memory 88 connected to the microprocessor 58 by a bus 90. The data comes via the handset antenna 11 and is downloaded through the contacts 18.

5 An alternative to countdown with the clock is to use pulses received from the network. In such an arrangement, during the course of a conversation, a pulse or other signal representative of unit of cost, is transmitted from the network to the telephone; and in accordance with those received pulses,
10 the prepaid units are removed from the prepaid card. In the GSM 11.11 standard, this is sometimes referred to as the "E parameter". It has seven variables, and is called an advice of charge protocol, AOC.

15 A clock 92 and power supply 94 is shown in Fig. 3 as being on the SIM chip. This is used for calculation of costs for a call made, and for generating with the microprocessor a signal or pulse to the prepaid card for decrementing the number of units remaining in the prepaid card register 32 in Fig. 2.

20 It should be understood that the clock 92 and the power supply 94 may be contained off the SIM and may be included in the handset. This is shown by the dotted line 96. Also, the SIM 8 need not be on a smart card, but may be permanently attached in the handset.

25 Typically, the two functions F and G and the diversification key Kd will be entered in the SIMs integrated circuit during manufacture. However, depending upon the manufacturing technique and the preferences of network operators, some or all of those items may be entered at a later stage of manufacture, e.g. after the IC is tested, and before
30 insertion in the card, or after insertion in the card, or after the card has been inserted in the network. Suitable security checks will be needed to install the two functions and

-27-

particularly the diversification key so that it cannot be read from the registers.

As used in this application, the contacts 14 and 18 are described as physical contacts on a surface of the card and in one embodiment are in accordance with the ISO standard. An alternative type of contact is that of a loop in which there is not a touching electrical contact with corresponding contacts inside the handset, but the contact is made electromagnetically through a coil in the card and in the handset. As the nature of contacts may develop over the life of this patent, the term contact as used herein and in the claims, covers all types of contacts which may be used to establish a connection, i.e. a transfer of data between the integrated circuit on the prepaid card, and the handset, and the integrated circuit in the SIM.

The present invention has been described with particular reference to a wireless or cellular telephone. The method, apparatus, integrated circuits and prepaid cards and SIMs of the invention are not so limited and may find other applications; for example, in subscriber pay-television, remote vending, electronic purse, reloading a pre-paid smart card.

Fig. 4 shows a cellular telephone handset 2 having a slot 4' to receive a removable SIM card 6', or to receive a removable prepaid card 8'. The SIM card and prepaid card meet the ISO standard cited above. It should be noted however, that one or both of the cards may be to the mini proposed ISO standard to other mechanical sizes. In operation, the cellular telephone 2 communicates through an antenna 11 with a cellular telephone network operator's station 12.

Fig. 5 is a highly schematic portrayal of the prepaid card 8'. The card has six or eight contacts 14 on one face, and an electronic circuit embedded in the card, which in current manufacture is a single integrated circuit 16'. The integrated

-28-

circuit is embedded in the card usually below the contact 14. According to the ISO standard, the card is 85 mm long, 54 mm wide, and 1 mm thick. The contacts 14 are eight in number or six as shown in Fig. 2, and occupy an overall area of not more than 2.62 mm x 9.32 mm. Each contact typically is not less than 1.7 x 2 mm. The contact area begins typically 10.5 mm from the left edge and 9 mm from the upper edge of the card. The integrated circuit 16' typically is 1 to 2 mm on each side, and a fraction of an mm thick.

Fig. 6 is a schematic view of the SIM card 6'. It is the same overall size and shape and with contacts 24' as the prepaid card 8. However, depending upon the internal circuitry in the handset, a contacts 24' on the SIM card 6' may be at a different location than on the prepaid card. There are provisions in the ISO standard for different locations of contacts. Alternatively, one set of contacts might be used in the handset, and the circuitry in the handset would decode whether it is a SIM card or a prepaid card. Slot 4' has the necessary connectors with contacts for making electrical connection to the contacts 14 and 24'.

On the first use of the hand set, the SIM is inserted into the slot and an exchange between the SIM and the network operator is initiated. This follows the usual protocol but with some exceptions, e.g., an inquiry is made to the user if this SIM is to be operated prepaid only, or if it can be both prepaid and a regular subscriber. If prepaid only, a flag is set in the SIM card shown with legend 26'. If it is to be a regular subscriber, then the usual credit check is provided until the user is identified, and an account is opened for the user, in which case the prepaid only flag 26' is not set.

If prepaid only, the SIM card is then removed, and the prepaid card 8' is inserted into the slot 4'. As shown in Fig.

-29-

5, the contacts 14 are connected through a bus 28' to a switch 30 on the integrated circuit. The integrated circuit includes a serial number of the prepaid card. Typically each prepaid card has a different serial number, which is stored in a serial number register 32'. A value, or number of prepaid units, is stored in a prepaid number of units register 34. A PLMN register 36' stores a list of numbers which identifies the networks in which the prepaid card may be used. This is to insure that a prepaid card for which money has been paid to one telephone system is used on the appropriate system. A certificate number for the card, which is computed based on a secret key, a sequence number, the prepaid number of units and the card's serial number, is stored in a certificate number register 38'. Text strings to be displayed on the handset text area are stored in a text string's register 40'. The registers 32'-40' are connected to the switch 30'.

The word registers as used in the description includes a specific location in memory, and a floating position or variable position within memory. It depends to some extent upon the sophistication of the integrated circuit as to how the different items, e.g. serial number, prepaid number of units, text string, PLMN list, and certificate number are stored. It should be understood that the register includes the various embodiments of how numbers may be stored in an integrated circuit and does not require the physical presence of a dedicated portion of memory in which to store each number. One designer may wish to design the circuit that way, and another might choose a floating, or variable, or other approach. The important point is that register, as used herein, identifies that the numbers can be stored, retrieved, and as appropriate, modified.

-30-

When the prepaid card is first inserted in the slot 4', the handset reads out through contacts 14 and switch 30', the PLMN number in register 36', and then a comparison is made either in the handset, or the PLMN number is sent to the network operator for comparison. If the number does not belong to the network operator's authorized list, then a text is displayed on the handset or another signal is given to the user that the prepaid card is not for use on this network.

If the PLMN number is authorized, then the serial number from the register 32', the prepaid number of units from register 34', and the certificate number from register 36' and a sequence number (which in the embodiment of Fig. 5, e.g. is 1, but in the embodiment of Fig. 10 is a changing number, all as described as more fully below) are uploaded temporarily to the handset. The prepaid card is marked as "read" by the handset (e.g. a flag is set on the card), and the card is then removed and the SIM card reinserted. The handset reads the IMSI number from the SIM and concatenates the IMSI with the prepaid number of units, the certificate number, and the sequence number, and uploads it to the network operator 12. The network operator then compares the serial number, the prepaid number of units, and certificate number (or may recalculate the certificate number from the serial and prepaid number of units) with corresponding information, which was previously and independently provided to the network operator from the card manufacturer and stored in the network operator's computer.

The text string register 40' may contain text to be read by the user, and which may be uploaded to the handset to be displayed during the initialization of the card or after verification. The text string might be advertisements or promotional material, and might include a game or bonus or

-31-

prize, etc. For example, the prepaid card might contain a bonus, similar to the rub-off prize bonus cards that sometimes accompany goods. This might be for 5, or 10, or some addition number of prepaid units of air time. If the card is a

5 "winner", then a display would be given to the user saying, "Congratulations!!! You have won 10 free units of air time." To use those bonus units, the prepaid card would include, for example, a second certificate number, and a second number of prepaid units, which might be stored respectively in registers

10 38' and 34'. If the user wished to use those units right away, he would leave the card inserted and initiate a procedure to transfer the units to the network operator, have them verified, and stored in the handset (temporarily to be subsequently transferred to the SIM), and the bonus units would then be

15 canceled from the prepaid card. Alternatively, the user might submit his bonus units later in another handset with another SIM. The important point is that where there is value to be given for the bonus, whether it is for additional air time units on the network, or to be used in another system, e.g. in

20 a public telephone system, or for purchasing in a vending machine, there is a corresponding certificate number, value, and if in a different system, a different system operator number, all of which must be on the card. As a further example of a bonus would be a message that says, "Take the card to the

25 ABC company, who will give you a prize of a particular prize." The ABC Company would then have equipment for verifying the certificate number and the fact that the bonus was in that card. The ABC Company, upon giving the prize would cancel the certificate number, or cancel the bonus entry from the card,

30 and from records at the ABC Company.

Referring now to Fig. 6, in the SIM card 6' the contacts 24 are connected through a bus 48 to the integrated circuit

-32-

which includes a switch 50, and a microprocessor 52. Signals to and from the card go from the contacts through the switch 50 to the microprocessor 52. Alternatively (not shown in the drawings), some signals might pass directly under control of the microprocessor via the switch 50 to registers in the card. Fig. 6 shows some structural elements in the SIM card which are additional in the present invention, and does not show all of those elements which are devoted to the routine GSM standard SIM card.

When the SIM card is reinserted into the handset, any difference between numbers in an accumulated call meter ACM register 54 and an accumulated call meter max ACM MAX register 56 is calculated and stored in ACM MAX. ACM is reset to zero. Then, the number of prepaid units taken from the prepaid card and validated by the network operator is added to ACM MAX register. ACM MAX defines the maximum number of units that ACM is allowed to reach prior to shutting down a call. Alternatively, if the ACM register and the ACM MAX register are used only for prepaid calls, the ACM register might be a continuous counter, i.e. never reset to zero, and the ACM MAX register also would be a continuous counter, and, the validated units would be added to ACM MAX. By setting ACM and ACM MAX, the network operator increases the amount of air time a customer is allowed to use and for which he has prepaid. The handset compares ACM and ACM MAX at the beginning of each call, and when each unit of air time is used. For a call to be initiated and to continue, ACM MAX must be greater than ACM.

In some systems, these two numbers for the ACM register and ACM MAX register may remain in the handset. If there were previous remaining ACM MAX units, then the ACM MAX register is updated. But, it should be noted, the updating is done by the network operator.

-33-

The handset does a comparison between the ACM register's contents and the ACM MAX register's contents, and if the ACM MAX register is larger, then a call may be made and continue. The prepaid only flag 26' is set by the network operator over the air, when the SIM is first used, and may be changed later by the network operator if the SIM goes on subscription.

It is not essential that the ACM register be set to zero, or that the ACM MAX register contain only the number of remaining prepaid units. Both registers might contain a continuous counter, or partial continuous counter, containing previous units expended. The exact details of when to reset the ACM register to zero and the ACM MAX register to the remaining units to be used, is a choice for the systems operator.

In a preferred embodiment of the present invention the instruction from the network operator to the handset and SIM to update the ACM register and the ACM MAX register passes over the short message service center SMSC, which is sometimes called the paging channel, and is encrypted. It is essential that this update message be encrypted, to avoid fraud on the system.

Fig. 7 is a schematic diagram of a portion of the network operator's computer. Added to the network operator's computer is a prepaid card data base 60' and additional elements in a supervisory control module 62. The data base 60' and control module 62' cooperate with other elements of the network operator's central office and which includes an O.T.A. platform 64' and a short message service center 66'. The various elements are shown schematically in a network operator's central office 70' having an antenna 72' and a switch 74'.

When the prepaid cards are manufactured (typically in lots of 100,000), a floppy disk or other memory which contains the

-34-

serial number of each card, the number of units on each card, and the certificate number of each card is sent to the network operator's central office, where it is entered on the card data base 60'. When the prepaid card is presented in the telephone handset, it must be validated and the card's serial number from register 32', the prepaid number of units in register 34' and the certificate number in register 38', and sequence number, and the IMSI of the SIM card are uploaded to the network operator 70' and a comparison is made with the corresponding data for that card, which has been entered in the central office card data base 60'.

If there is a match with the card and the data base, then an executable short message request is sent to the short message service center 66' via the O.T.A. platform 64'. The executable short message contains instructions to increase ACM MAX register 56 by the number of units taken from the prepaid card, and set ACM register 54' to zero, or as described above. The executable message also may contain a text string for display of a short message. This could read, e.g. "The value of \$20.00 has been accepted by the network." This executable message could also be returned via a USSD to the attention of the IMSI.

A record of use for that particular card is made. E.g. the serial number and/or certificate number of the card which has just been read is marked as "read" in the card data base 60', thus making it impossible to use its certificate number again. Preferably the records marked as "read" will be deleted from the card data base during the next new data load, or at any other convenient or conventional time.

The SIM card 6' receives the executable short message and updates its ACM MAX register 56 (by the number of new units

-35-

plus the difference between old units in ACM and ACM MAX), and resets ACM register 54 to zero.

To minimize fraud on the system, there is included in the supervisory control module 62' for each SIM which has prepaid units, an ACM register 75 and an ACM MAX register 76'. There are two such registers 75 and 76' for each SIM on the system having prepaid cards. The ACM and ACM MAX registers 75 and 76' have duplicate information as to what is in the corresponding ACM and ACM MAX registers of the corresponding SIMS.

At the beginning of each call, if that SIM is to operate on prepaid only, the supervisory module 62' validates that the presence of units in the ACM MAX register 76' for that card is greater than the units in ACM register 75 for said card. If validated, the call is set up, and the network provides a start time to the supervisory control module 62. As the call progresses, the supervisory control module increases (or decreases depending upon how the system operates) the number in the ACM register 75. For each time unit, a comparison is made with the number in the ACM MAX register 76'. Substantially simultaneously, but independently, as the call progresses, the ACM register 54 is increased (decreased if the system operates that way) in the SIM card 6'. If the call progresses beyond either the number of units provided by ACM MAX register 56 as monitored by the handset; or as monitored on the supervisory control module 62', 75 and 76', then the call is interrupted. If first detected on the handset, then the handset notifies the network that the call is becoming invalid, and that there are no more prepaid units, or credit. If first detected on the supervisory control module, a similar signal is generated. The network, depending upon the choice of the network operator, would discontinue the call, but might send a notice or warning signal to the user, one or two units before expiration, that a

-36-

new card needs to be inserted, and that only one or two units remain. The call might be transferred to an operator, or to a robotic voice advising that additional units need to be inserted, or a different payment substituted. The important point is that both the handset and the supervisory control module independently keep track of the call as it progresses.

At the end of the call, or at other times, the ACM and ACM MAX register in the SIM card can be compared with the values in the ACM and ACM MAX registers 75 and 76' for that SIM card in the supervisory control module.

In an alternative embodiment, the central office does not continuously monitor remaining value in the card, but only the beginning and end of a call. This leaves in the central office and the supervisory control module the number of units or air time remaining. Here, when the number of units or air time remaining is exceeded, i.e. the ACM = ACM MAX on the SIM card, then the handset sends a signal to the central office to interrupt the call. The fact that the call is interrupted may also be recorded on the supervisory control module 62'.

To perpetrate a continuous fraud on the network the service control module 62' would have to be tampered with, which is outside the reach of most perpetrators. As an alternative, calls need not be monitored from the central office supervisory control module for each unit of call, but might be for every several units of calls, or for a given period of time. Thus, a user might get a short "free" use of the phone, but not any subsequent calls after the number of prepaid units have been exhausted.

An aspect of applicant's invention is to download from the supervisory control module 62' to the ACM and ACM MAX registers of the SIM card through the short message service center 66' an

-37-

executable short message, which is an encrypted and secure transmission channel.

Fig. 8 is a flow chart illustrating one embodiment of validation of a prepaid card, and entry of validated prepaid units in the SIM card and in the supervisory control module. As shown in block 80', the SIM card, if in the handset, is removed, then the prepaid card is inserted. The handset interrogates the prepaid card and determines if one of the PLMN numbers read from the PLMN register 36' in the card matches the PLMN number of the network in which the handset is operating. If there is no match, then a display on the handset indicates to the user that the card is for another network. The message may be displayed visually or by voice. If the PLMN number does match, then the handset interrogates the prepaid card as shown in block 84' if there are prepaid units in register 34' of the card. If there are none, then the display indicates that the card has been used up or that no units are available. If there are, the validation proceeds, a flag is set in the prepaid card that the units are used, and the serial number, prepaid number of units and the certification and sequence number are read out of the card, uploaded from the card to the handset, as shown in block 86. There may be at this point a display on the handset to say, "remove prepaid card, & reinsert SIM card" and then, "Please wait. Your card is being uploaded," or other message. After the SIM is reinserted 87', the handset then uploads as shown in block 88' to the network operator 70' information about the prepaid card and the SIM card particularly the IMSI of the SIM. As noted, this may either be an anonymous IMSI where the cellular phone is to be used only with prepaid cards, or may be a regular subscription IMSI. Also sent to the network operator is the certificate number of the prepaid card, the sequence number, and the number of units in the prepaid

-38-

card which are to be used. The central office then compares the certificate number and the number of units with the certificate number and the number of units for that card in the card data base 60'. As shown in block 90', the central office compares the certificate number and the number of units in the card, and determines whether it agrees with the certificate number and number of units for that card in the card data base 60'. If there is no agreement, then a signal 91' is sent back to the handset, which causes a message to appear on the display that the card cannot be validated. If there is an agreement in step 90', then two events occur. First is in the network operator, and is shown in block 92'. Here, the number of the card, which has just been validated, its certification number and perhaps the number of units for this card, are erased from the card data base 60'. Second, in the supervisory control module, the ACM register 74' corresponding to this card is set to zero, and the ACM MAX register for this card 76' is increased by the number of units taken from the card set to the number of units taken from the card and the previous remainder between ACM MAX and ACM. The second event is the downloading via the executable short message to the SIM, which is shown here with block 94'. The display then gives a message that the card has been validated. In the SIM card, the ACM register 54 is set to zero, and the ACM MAX register now has the number of units that have been removed from the prepaid card plus any remainder from before.

Fig. 9 is a flow chart showing a call approval routine for calls from a cellular telephone, which has validated prepaid units stored in the SIM card 6', and corresponding prepaid validated units registered in the central office supervisory control module 62'. A call originates as shown in block 100. An interrogation is made in the handset as shown on

-39-

interrogation block 102, is the prepaid only flag 26' in the SIM card set? If there is no flag, then the call proceeds as a normal subscription, or there is limited access, e.g. 911, to an operator as shown in box 104. If yes, then the handset proceeds to interrogation as shown in box 106 to determine is there prepaid value, and a comparison is made between the contents of the ACM Reg 54 and ACM MAX Reg 56. If there is no value remaining, then a message is sent to the supervisory control module, and a display to the user. If there is value left, then the call is initiated 108.

An inquiry is made to the supervisory control module 62' as shown in question box 110 where a comparison is made between the ACM register 74' and the ACM MAX register 76' for this SIM card. If the ACM MAX is greater than ACM, then the call proceeds as shown in box 111. A clock 112 times the call. This clock may be operated from the network operator or located in the handset. As each unit of air time is used, the ACM 54 register in the SIM card in the handset, and the ACM 74 register in the supervisory control module is increased. This is shown by blocks 114 and 116. The comparison is repeated, shown at 110A, an 110B, as the call continues. As each unit expires, a comparison is made and if ACM is less than ACM MAX, then the call continues, as shown in block 111. When the ACM reaches the ACM MAX, whether it is in the handset or in the network operator's office, a signal is sent to interrupt the call as shown in block 118. Alternatively, the loops are interrupted, when the user completes the call. At that time, there may be a handshake between the ACM and the ACM MAX registers in the SIM card with the corresponding registers in the security control module. In the event of a discrepancy (defined here as a difference of more than one unit), there is a report generated to the network operator. For handling

-40-

fractional seconds, a protocol should be worked out with the network operator as to which counter would take precedence. The two ACM's and two ACM MAX's should at all times agree.

If the call continues, when $ACM = ACM\ MAX$, there is an interruption in the call. A display may also be made on the handset. At the end of a call, the remaining value, i.e. the difference between ACM and ACM MAX, may also be displayed on the handset. A similar display may be made at the time the handset is powered up.

Fig. 10 is a schematic drawing of a prepaid card showing an alternative embodiment of a prepaid card in which some, but not all of the prepaid units may be transferred from the prepaid card to the SIM and the network operator's supervisory control module.

In Fig. 10, as with elements in Fig. 5, the card 8' has the contacts 14, and the bus 28' connected to the switch 30'. In addition to the serial number register 32', prepaid number of units register 34', PLMN register 36', certificate number register 38', and text string register 40', there is a sequence number register 46, and a microprocessor 128, which communicates with the switch 30'. A sequence number is held in the sequence register 46. When a card is first shipped, the register is set to "1". The certificate is calculated with the sequence number of "1". When the card is used the first time, the sequence number goes to the next number, e.g. "2", and a new certificate is calculated. This continues, each time a new certificate is calculated, until all of the prepaid units are used. For cards, such as those shown in Fig. 5, which cannot be partially used, i.e. all of the units must be taken out at one time, there is no sequence number register, and for encryption the sequence number is e.g. "1". It will be appreciated that another number than "1" might start the

-41-

sequence, and the number "1" is used for purposes of illustration only; also, the sequence might be a multiple string of numbers.

The switch 30' and microprocessor 128 can be combined on the integrated circuit. Some or all of the functions performed by the switch might be performed internally in the microprocessor.

In Fig. 10 some but not all of the prepaid number of units may be transferred to the SIM ACM MAX register 56 and the card data base supervisory control module ACM MAX register 76', while calculating and leaving a certificate number in the card 8' and a reduced number of prepaid units in the prepaid unit register 34'.

Prepaid card 8' has information which is readable outside of the prepaid card, namely the number of units remaining in the card and the serial number of the card. Invisible in the card, i.e. it cannot be taken out of the card, is a functional algorithm F shown in a function register 135 and a key for that algorithm Kn, shown in register 137. When the card is originally manufactured and shipped, the certificate number for the card, the prepaid number of units, the card number, a key, and sequence number are transmitted to the network operator. When the card is first placed into use, it is verified. At that point, a question is put to the user as to the number of units to be added to ACM MAX registers. If the user takes less than all of the prepaid number of units in register 34, then that number of units selected is placed in ACM MAX registers. The prepaid card 8' in its microprocessor 128, recalculates a new certificate number using the algorithm F and the key number Kn and sequence number Seq. Nb. The new certificate Cert1 is then stored in the certificate no. register 38' and the sequence number is increased by one. An independent

-42-

calculation may be made in the supervisory control module 62' and placed in the card data base 60'. There is a handshake or verification of the Cert1 # as it appears in the prepaid card 8' and in the updated card data base 60'. The card data base
5 contains not only the new certificate number Cert1 but also the number of remaining prepaid units for this card. The new certificate number and number of units remaining, of course, is transmitted over an encrypted and secure transmission. Variations might include calculating new certificate number
10 Cert1 only in the card, and then copying to the supervisory control module and card data base.

In summary, for this embodiment the user has the option to transfer only a portion of the prepaid units to the SIM. The card calculates a new certificate number using, the number of
15 units, the function F and key number Kn and sequence number Seq. Nb. The new certificate Cert1 is concatenated with the IMSI of the SIM and sent to the network operator.

When a card in this embodiment is used, the supervisory control module for such prepaid card does not need to store the
20 certificate numbers. It calculates the certificate number by having the card serial number, the number of units uploaded, the sequence number, and the key Kn. The supervisory control module has the algorithm. This provides an extra level of security in that there may be a parallel and independent
25 calculation of each new certificate number for the remaining value for the prepaid cards.

In this embodiment, when a card having only a portion of the units used, is presented to use the remaining number of units, then the network operator first searches the card data
30. base for the original certificate number. If this is not found, the card data base does a reverse calculation of certificate numbers to determine if a valid Cert1 has been

-43-

entered. Alternatively, it might go directly to a data base of Cert1 numbers.

Another aspect is when a SIM card is in a subscription mode, i.e. the prepaid only flag 26' is not set, a prepaid card
5 may still be used. For example, if a person borrows another's cellular telephone, then the borrower may use his prepaid card to pay for some, all, or more of his telephone call. The borrower could insert into the handset a prepaid card, with for example a \$5 value. This prepaid card, for example of the type
10 shown in Fig. 5, would then be read and uploaded through the handset to the network operator's central office where the supervisory control module would interrogate the card data base. The card after validation would then transfer the value of that card to the lender's subscriber's accounts, i.e. the
15 SIM subscription for a credit. This would appear on the bill of the subscriber.

A second example is a promotional prepaid card sent to a person having a regular subscription. The card would be inserted into the handset for which the SIM operates in a
20 subscription mode. The prepaid card would be uploaded through the handset, and validated. The card would be marked "USED", or a flag would be set that the card has been used. And, the subscriber would have a credit to his subscription account, or telephone bill, for the amount of the prepaid card.

25 It will be apparent, therefore, that the illustrative embodiments described are only examples and that various modifications can be made in the construction, method and arrangement within the scope of the invention as defined in the appended claims.

Claims:

1. A method for enabling service from a wireless telephone having a SIM and a prepaid card in the telephone comprising the steps of:

5 (a) calculating in the card a certificate as a function of

(i) number of prepaid units remaining in the card,

(ii) serial number in the card, and

(iii) a key number in the card;

10 (b) transferring from the card to the SIM

(i) said number of prepaid units remaining in the card, and

(ii) the card's serial number;

(c) calculating in the SIM a number which should be the same as the card key number based on said transferred number of prepaid units remaining in the card and said card serial
15 number;

(d) calculating in the SIM a certificate as a function of said transferred number of prepaid units remaining in the card and said calculated number which should be the same as said key
20 number in the card;

(e) comparing said calculated certificates from said card and from said SIM; and

(f) if coincident in said comparison then enabling said telephone in said network.

25 2. The method of claim 1, wherein said calculations of said certificates in said card in step (a) and in said SIM in step (d) use the same algorithm.

30 3. The method of claim 1, wherein said calculation in step (c) of said number which should be the same as said card key number, uses a diversification key which is the same in a plurality of wireless telephones serviced by one network operator.

-45-

4. The method of claim 1 or 3, wherein said key number comprises a first sequence which is unique for each card, and a second sequence which is common to a plurality of cards and unique for each network operator.

5 5. The method of claim 1 or 2, wherein one of said calculations of said certificates and said calculation of said key number which should be the same as the card key number employ different algorithms.

10 6. The method of claim 1, further comprising the steps of

(g) storing rate information in the telephone;

(h) measuring time usage after said telephone is enabled in the network and said telephone is placed in use for measuring time said telephone is in such use; and

15 (i) decreasing the number of remaining prepaid units in said card in accordance with the rate information and said time usage of the telephone.

20 7. The method of claim 6, wherein said decreasing step generates a periodic signal, with a period of said periodic signals corresponding to a prepaid unit, and said period is a function of said telephone rate information stored in said telephone, and a function of a type of service selected by a user of the telephone.

25 8. The method of claim 1 wherein said SIM generates a random number, transferring said random number to said prepaid card, and wherein said certificates calculated in said card and in said SIM each include as a function thereof said random number.

30 9. The method of claim 6, wherein said storing is in said SIM, and further comprising the step of modifying said rate information in said SIM by incoming wireless transmission from said network.

-46-

10. The method of claim 1, wherein said enabling signal changes said telephone from a restricted mode of use to a less restricted mode of use.

11. The method of claim 6 or 7 comprising in said
5 decreasing the number of remaining prepaid units in said card further comprises steps of

- (j) generating a random number in said SIM;
- (k) transferring said random number to said card;
- (l) recalculating said certificate in said card as a

10 function of

number of units now remaining in the card,
said serial number of the card,
said key number of the card, and
said random number;

15 (m) recalculating a certificate in said SIM as a function
of

said number of units now remaining in the card,
said serial number of the card,
said key number of the card, and
20 said random number;

(n) comparing said recalculated certificates and if non-coincidence then

- (o) disabling said telephone from said network.

12. The method of claim 11, comprising the steps of
25 repeating said steps (j) - (n) for each unit decreased from said card.

13. The method of claim 11, wherein said recalculating in said SIM comprises two sub-steps,

30. first generating in the SIM a card key number based on said transferred number of units remaining in the card and the serial number of the card which generated number should be the same as the key number in the card, and

-47-

second calculating in the SIM from said just generated card key number, and from said random number, and from said number of units now remaining in the card, said recalculated certificate.

5 14. An apparatus for enabling service from a wireless telephone having a SIM and a prepaid card in said telephone comprising:

(a) means for calculating in the card a certificate as a function of

10 (i) number of prepaid units remaining in the card,
(ii) serial number in the card, and
(iii) a key number in the card;

(b) means for transferring from the card to the SIM

(i) said number of prepaid units remaining in the card, and
15 (ii) the card's serial number;

(c) means for calculating in the SIM a number which should be the same as the card key number based on said transferred number of prepaid units remaining in the card and said card serial number; and

20 (d) for calculating in the SIM a certificate as a function of said transferred number of prepaid units remaining in the card and said calculated number which should be the same as said key number in the card

(e) means for comparing said calculated certificates from
25 said card and from said SIM, and if coincident in said comparison then enabling said telephone in said network.

15. The apparatus of claim 14, wherein said means for calculations of said certificates in said card and in said SIM use the same algorithm.

30. 16. The apparatus of claim 15, wherein said means for calculation of said number which should be the same as said card key number comprises a diversification key which is the

-48-

same in a plurality of wireless telephones serviced by one network operator.

17. The apparatus of claim 14 or 16, wherein said key number comprises a first sequence which is unique for each card, and a second sequence which is common to a plurality of
5 said cards and unique for each network operator.

18. The apparatus of claim 14, further comprising
means for storing rate information in the telephone,
means for timing said telephone when in use, and
10 means for decreasing the number of remaining prepaid units in said card after said telephone is enabled in the network and said telephone is in use, in accordance with the stored rate information, and time duration of telephone use.

19. The apparatus of claim 14, further comprising
15 means for storing rate information in the telephone,
means for generating a periodic signal, wherein a period of said periodic signals corresponds to one of said prepaid units, and said period is a function of said telephone rate information stored in said telephone and time duration of
20 usage of said telephone when enabled, and new line means for decreasing the number of remaining prepaid units in said card in accordance with said pulses.

20. The apparatus of claim 18 or 19, comprising means for modifying said stored rate information upon receipt of incoming
25 wireless transmission of rate information from said network.

21. The apparatus of claim 18 or 20 comprising
(a) means for generating a random number in said SIM;
(b) means for transferring said random number to said
card;

30. said means for calculating in said card including means for recalculating said certificate in said card as a function of

number of units now remaining in the card,
said serial number of the card,
said key number of the card, and
said random number;

(d) said means for calculating a certificate in said SIM
including means for recalculating a certificate as a function of
said number of units now remaining in the card,
said serial number of the card,
said calculated key number of the card, and
said random number;

(e) said means for comparing including means for comparing
said recalculated certificates and if non-coincidence then
disabling said telephone from said network.

22. A smart card, which in normal use in a network allows
the transfer of goods/services to a user of the card from a
network operator by subtracting prepaid units of value stored in
said card in exchange for said goods/services comprising a card-
shaped carrier having a terminal and an integrated circuit
embedded in said carrier and connected to said terminal; said
integrated circuit comprising

a serial number register for storing a serial number unique
to each card,

a prepaid units register for storing a number of units of
prepaid value,

a switch responsive to interrogation at said terminal to
write to said terminal said serial number in said serial number
register, and to write to said terminal said number of prepaid
units remaining in said units register,

a key number register storing a key number, which has a first
portion unique for each card, and a second portion which is common
to a plurality of cards, and which is unique for a

-50-

network operator, said key number in normal use of said card not being readable at said terminal,

an algorithm stored in said card, said algorithm in normal use of said card not being readable in said terminal,

5 a microprocessor for calculating a certificate in accordance with said algorithm as a function of said key number and the number in said prepaid register, and said certificate being readable at said terminal.

10 23. A smart card, which in normal use in a network allows the transfer of goods/services to a user of the card from a network operator by subtracting prepaid units of value stored in said card in exchange for said goods/services comprising a card-shaped carrier having a terminal, and an integrated circuit embedded in said carrier and connected to said terminal;

15 said integrated circuit comprising

a serial number register for storing a serial number unique to each card, and which number in said register in response to interrogations at said terminal being readable at said terminal,

20 a prepaid units register for storing a number of units of prepaid value, and which number in said units register, in response to interrogations at said terminal being readable at said terminal,

25 a key number register storing a key number, which has a first portion unique for each card, and a second portion which is common to a plurality of cards, and which is unique for a network operator, said key number in normal use of said card not being readable at said terminal,

an algorithm stored in said card, said algorithm in normal use in said card not being readable in said terminal,

-51-

a microprocessor for calculating a certificate in accordance with said algorithm as a function of said key number and the number in said prepaid register, and said certificate being readable at said terminal.

5 24. A subscriber identification module for operating with prepaid cards and with a network that provides goods/ services via said network comprising

an integrated circuit having,

(a) an input for receiving from one prepaid card

10 (i) a serial number of said card,

(ii) a number of prepaid units remaining in said card,

and

(iii) a certificate compiled by said card from its serial number, card key number, algorithm, and number of prepaid units remaining in said card;

15 (b) a diversification key which is the same for a plurality of modules of a network;

(c) first and second algorithms;

(d) a microprocessor for calculating

20 (i) a card key number with said first algorithm as a function of said diversification key, and said receive serial number of said card, and where said calculated card key number should be the same as said key number in said card; and

25 (ii) calculating a certificate with said second algorithm as a function of said calculated card key number, and said receive number of prepaid units remaining in said card; and

(iii) comparing said calculated certificate with said received certificate, and

30 (iv) if coincidence, generating an enable signal whereby goods/services are provided in accordance with said generated enable signal.

RECTIFIED SHEET (RULE 91)
ISA/EP

25. The module according to claim 24 further comprising
 (a) a clock input;
 (b) a register for receiving and storing time/ tariff
rates of the goods/services provided via the network;
5 (c) an output for sending signals to said prepaid card;
 (d) said microprocessor calculating cost of a unit of
goods/services as a function of
 (i) time elapsed via said clock input, and
 (ii) the rates stored in said register, and
10 (e) in accordance with said calculations generating a
signal on said output, representing consumption of a prepaid unit,
whereby said output signal decreases the number of prepaid
units in said card.

26. The module according to claim 24, wherein said
15 diversification key is the same for a plurality of modules and is
unique to a network, and said card key comprises a portion which
is unique for each card and another portion which is unique to a
network.

27. A device according to any one of claims 14, 22, 23 or 24
20 wherein said SIM generates a random number and transfers said
random to said prepaid card and said calculations of said
certificates comprise said random number as an additional
variable.

28. The apparatus according to claim 18, wherein said stored
25 rate information is selected from the group consisting of a table
look-up and a formula.

29. A method for prepaid cellular telephone calling with a
prepaid card comprising the steps of

(a) validating a number of prepaid units of a prepaid card;

-53-

(b) recording said number of validated prepaid units in a SIM, said SIM to be used in a cellular telephone, and also recording said number of validated prepaid units at a network operator;

5 (c) calculating the number of prepaid units as a call progresses at two separate locations with said calculations being done independently, one being associated with the SIM and the other in the network operator, and

10 (d) interrupting a call-in-progress, when either of the calculations shows no remaining prepaid units.

30. The method of claim 29, wherein said validation comprises

(i) determining if said prepaid card is for service with the network operator;

15 (ii) transmitting from said prepaid card to the network operator a number of units to be validated from said card and a certificate number of that card; and

20 (iii) comparing in the network operator said certificate number and said number of units transmitted from said card, with a certificate number and a number of units for said cards independently received by the network operator.

31. The method of claim 29, wherein said recording comprises

25 (i) having a first meter in said SIM and a first meter in said network operator, both of said first meters set to a predetermined number of units; and

(ii) setting a second meter in said SIM and second meter in said network operator to a number of units different from said number of units in said first meters each by an amount including said number of validated prepaid units.

30 32. The method of claim 31, wherein said calculating comprises

RECTIFIED SHEET (RULE 91)
ISA/EP

-54-

(i) increasing said number of units in both said first meters in accordance with air time usage of said telephone; and

(ii) comparing said number of units in said first and second meters in said SIM and comparing said number of units in said first and second units at said network operator.

33. A wireless telephone network comprising

(a) equipment for operating a wireless telephone network of wireless telephones according to a protocol,

(b) a card data base comprising information on a plurality of prepaid cards which are to be used in wireless telephones on the network, said data base comprising for each card to be used in the network

(i) a serial number of the card,

(ii) a number corresponding to units of prepaid telephone calls,

(iii) a certificate number which is a function of the card's serial number and number of units,

(c) a supervisory control module for validating each card when first used on the network by comparing the card's certificate number as received from a wireless telephone having the prepaid card therein, with the corresponding numbers for said card stored on the card data base,

(d) apparatus for

(i) downloading a message to said wireless telephone that units are transferred from said card to said telephone; and

(ii) for sending a signal to said data base that the number of units associated with said card number has been used, and is no longer available.

34. A mobile telephone handset comprising

(a) telephone circuitry to communicate with a wireless network operator in accordance with a protocol;

RECTIFIED SHEET (RULE 91)
ISA/EP

-55-

(b) a slot for receiving a removable SIM card;

(c) said slot also accepting and reading a removable prepaid card having

(i) a serial number,

(ii) a number corresponding to units of prepaid telephone time,

(iii) a number corresponding to the network in which the card may be used, and

(iv) a certificate number which is a function of the serial number and the number of units;

(d) said SIM card including a storage whose contents correspond to prepaid units remaining available to be used for calls, and a flag indicating if a telephone call is to be paid with said prepaid units.

35. A telephone handset in accordance with claim 34, wherein said flag indicates if the calls may only be placed against prepaid value, whereby for a call to be made either said flag must be set and there are validated prepaid units in the SIM, or said flag is not set and the SIM card and network operator accept the call is on a subscription basis.

36. A data disk for use in a mobile telephone network, which provides for prepaid cards on the network and in which a number corresponding to value of prepaid calls is stored on cards and transferred to telephone handsets operable on the network,

said data disk comprising

(a) identification numbers of each card with prepaid value which may be used on the network,

(b) a number representing the value of prepaid calls stored on each card, and

RECTIFIED SHEET (RULE 91)
ISA/EP

(c) a signature of each card, said signature being a function of the card's identification number and number of units; whereby said data disk being readable at the network operator and the data thereon being storable at said network operator for use in accepting and keeping records of said prepayments and calls placed against said prepayment.

37. The disk according to claim 36, wherein said signature further is a function of the network operator identification number.

38. A pre-paid chip card for use in a mobile telephone handset in a mobile telephone network, said card comprising an integrated circuit having

(a) a memory and stored therein
(i) a first number representing a serial number of the card;

(ii) a second number representing value of prepaid telephone calls to be made from a mobile telephone;

(iii) a third number representing a mobile telephone network in which said card may be used;

(iv) a fourth number representing a certificate, which is a function of said first and second numbers;

(v) a message string which is to be displayed on a mobile handset after said card is inserted in said mobile telephone handset;

(b) circuitry operable in response to signals from said handset for enabling said numbers from said memory to said handset when said card is inserted into said mobile telephone handset, and for enabling said message string to be displayed on said handset.

39. The card according to claim 38, wherein said signature is also a function of said third number.

40. The card according to claim 38, further comprising in said integrated circuit a microprocessor having an algorithm, a key, and a sequence number generator.

41. A method of operating a mobile telephone system with prepayment in which the system has

5 a network operator,
a plurality of handsets each with a removable SIM card,
a plurality of prepaid cards each with prepaid units, and a certificate,

10 comprising the steps of

(a) removing the SIM card from the handset and replacing the SIM card with a prepaid card,

(b) entering from the prepaid card into the handset,

15 (i) a number of prepaid units and
(ii) the certificate number,

(c) transmitting from the handset to the network operator the number of prepaid units entered from the card and the certificate number entered from the card, and

(d) verifying at the network operator the validity of the

20 number of units and the certificate received from the handset, and if correct, then transmitting to the handset a message for increasing in the SIM card an accumulated call meter max by the number by said number of units as verified by the network operator.

25 42. The method of claim 41, further comprising in step (b) after entering the units to the handset, then marking said prepaid card that said prepaid units have been used.

43. The method of claim 41 further comprising when a call is subsequently made using said SIM the steps of

30 (g) debiting an accumulated call meter in said SIM card for each unit of air time,

(h) comparing said accumulated call meter with said accumulated call meter max,

(i) permitting said call to continue as long as said ACM is less than ACM MAX, and signaling the network operator for interrupting said call when said ACM value is at ACM MAX,

whereby a call continues as long as credit remains between ACM and ACM MAX and charge for the call takes place within the SIM, and handset, without each unit of call being cleared back and forth with the network operator.

44. The method of claim 43, further comprising at a beginning and an end of each call transmitting from the handset to the network operator the number of units in ACM, and in ACM MAX, and storing said numbers at the network operator.

45. The method of claim 44, further comprising when a call is initiated verifying the ACM and ACM MAX number, of units in the SIM before permitting a call from that SIM to continue.

RECTIFIED SHEET (RULE 91)
ISA/EP

1 / 7

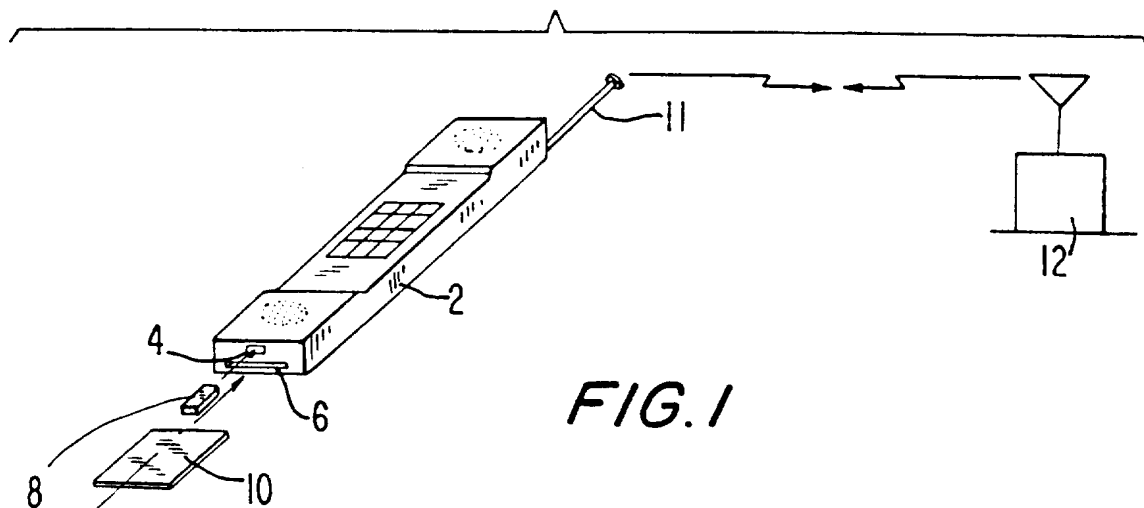


FIG. 2

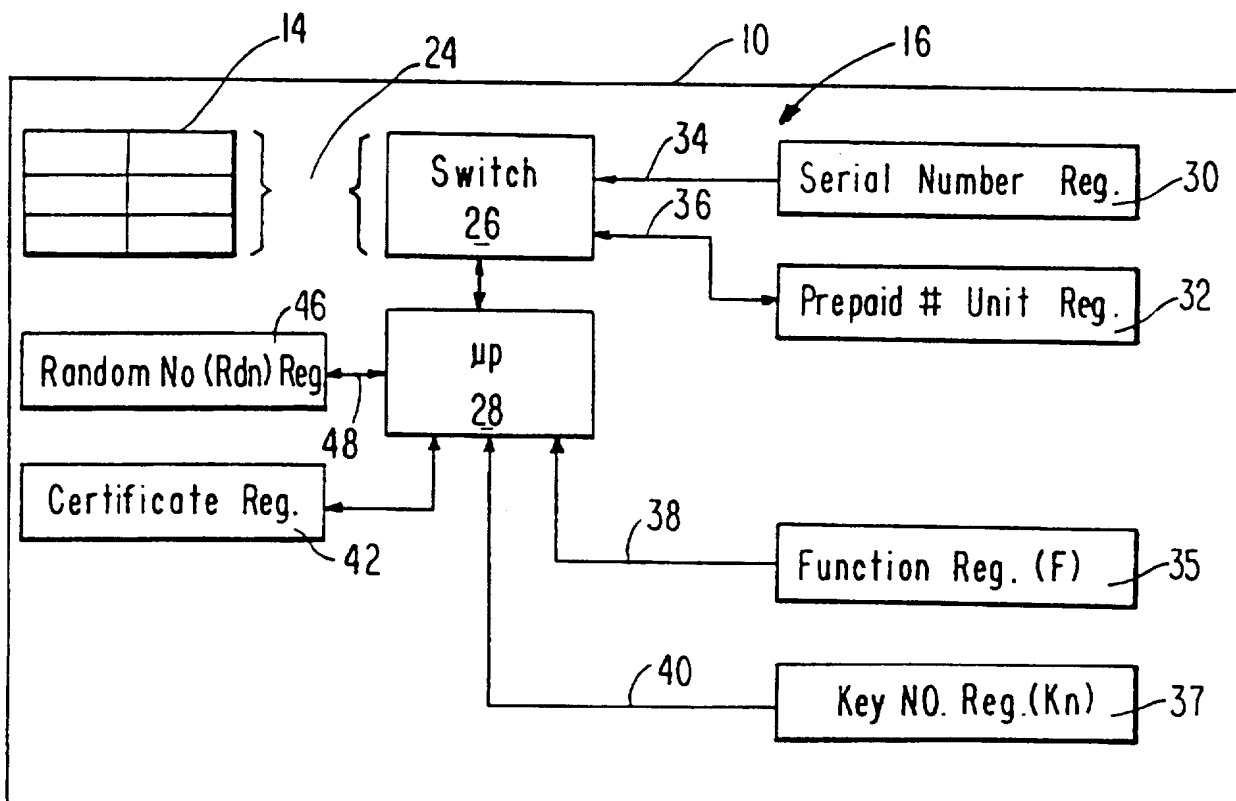
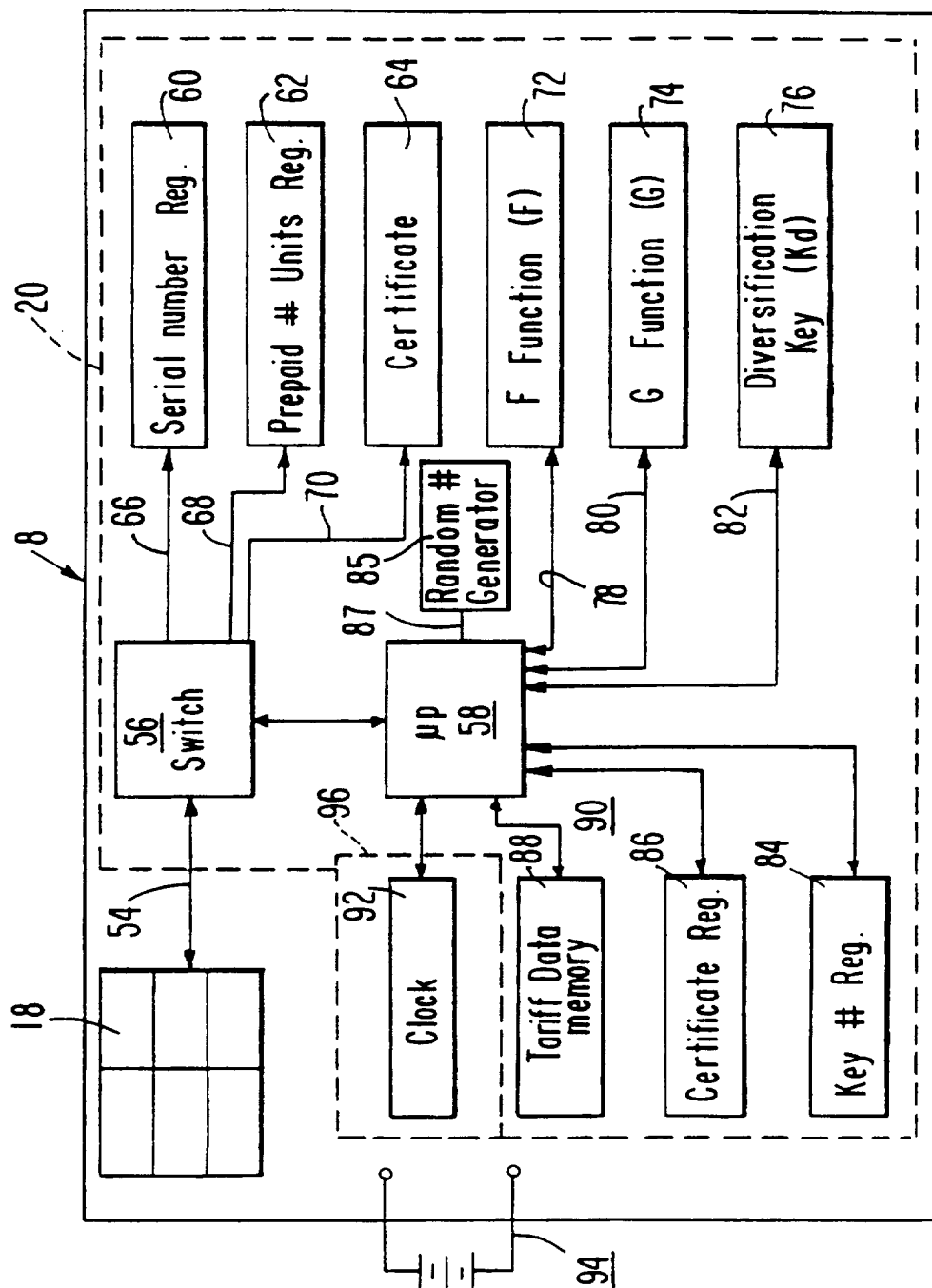


FIG. 3



3/7

FIG. 4

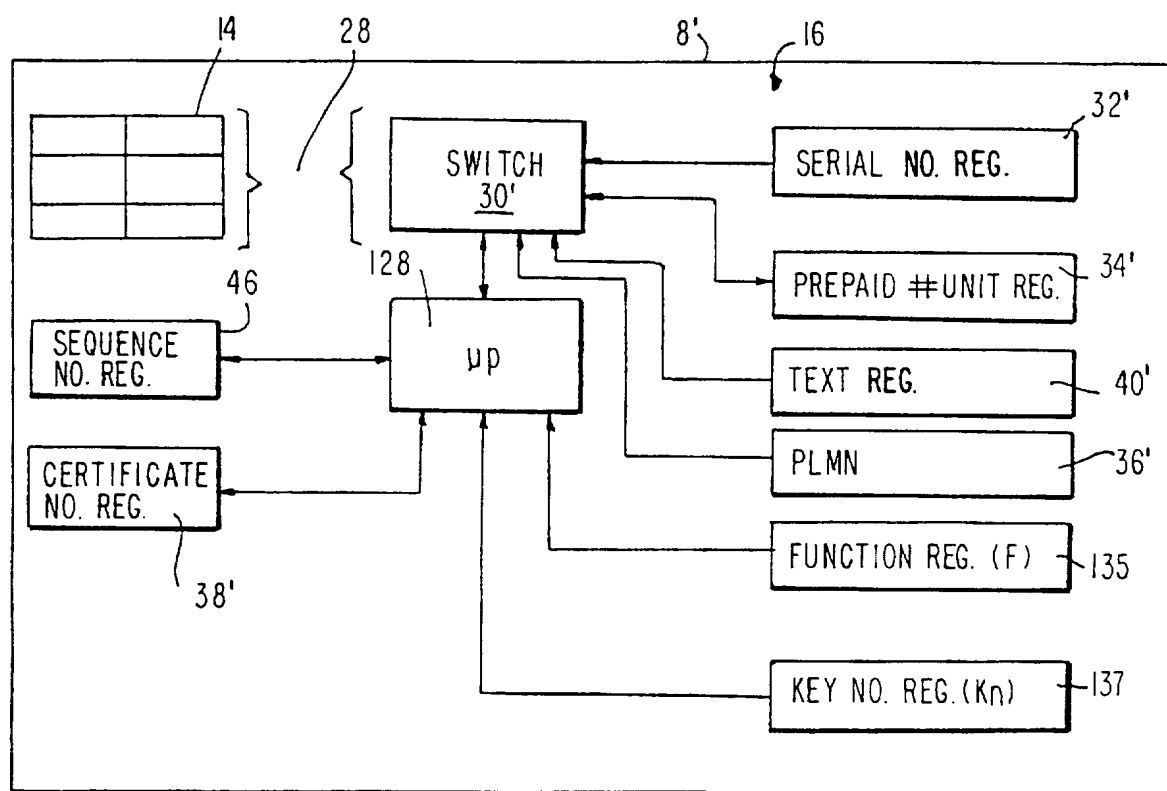
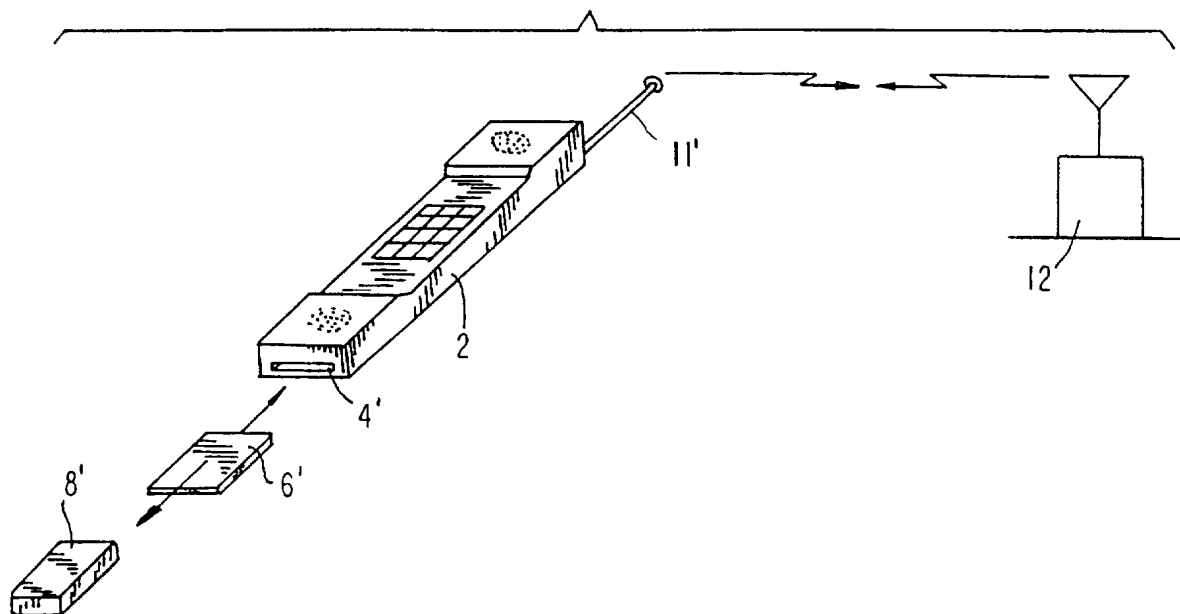


FIG. 10

4/7

FIG. 5

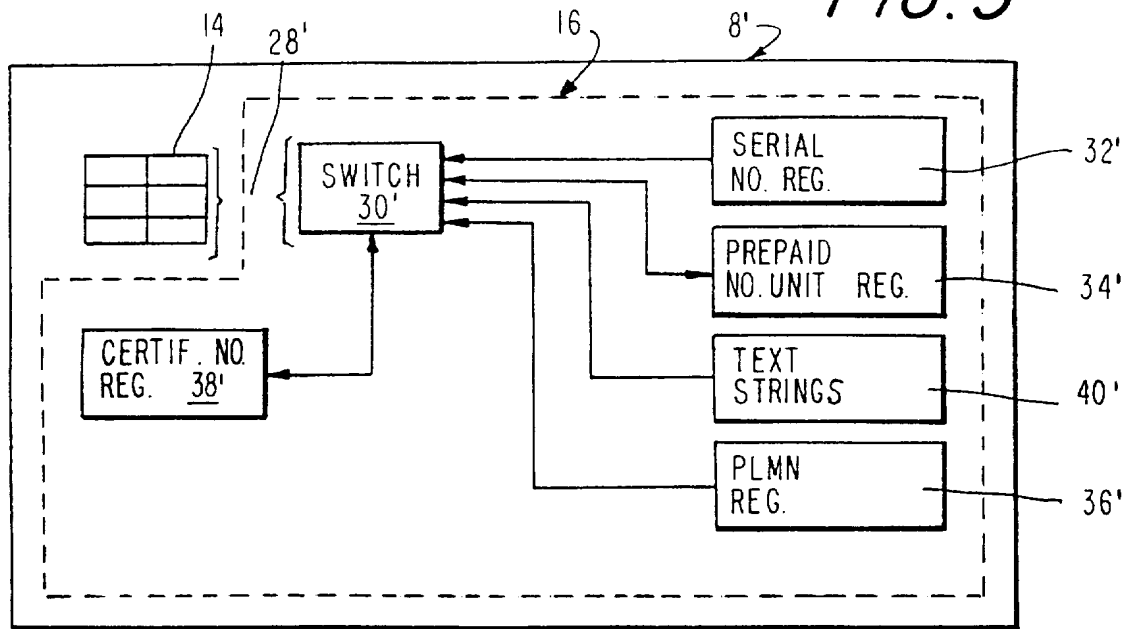
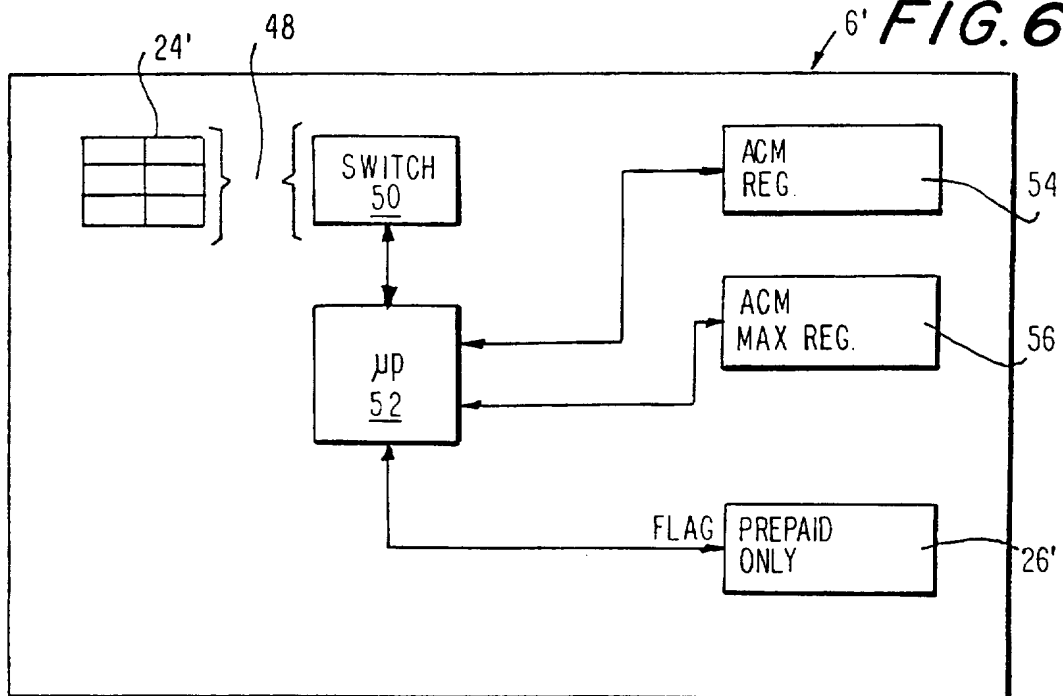


FIG. 6



5 / 7

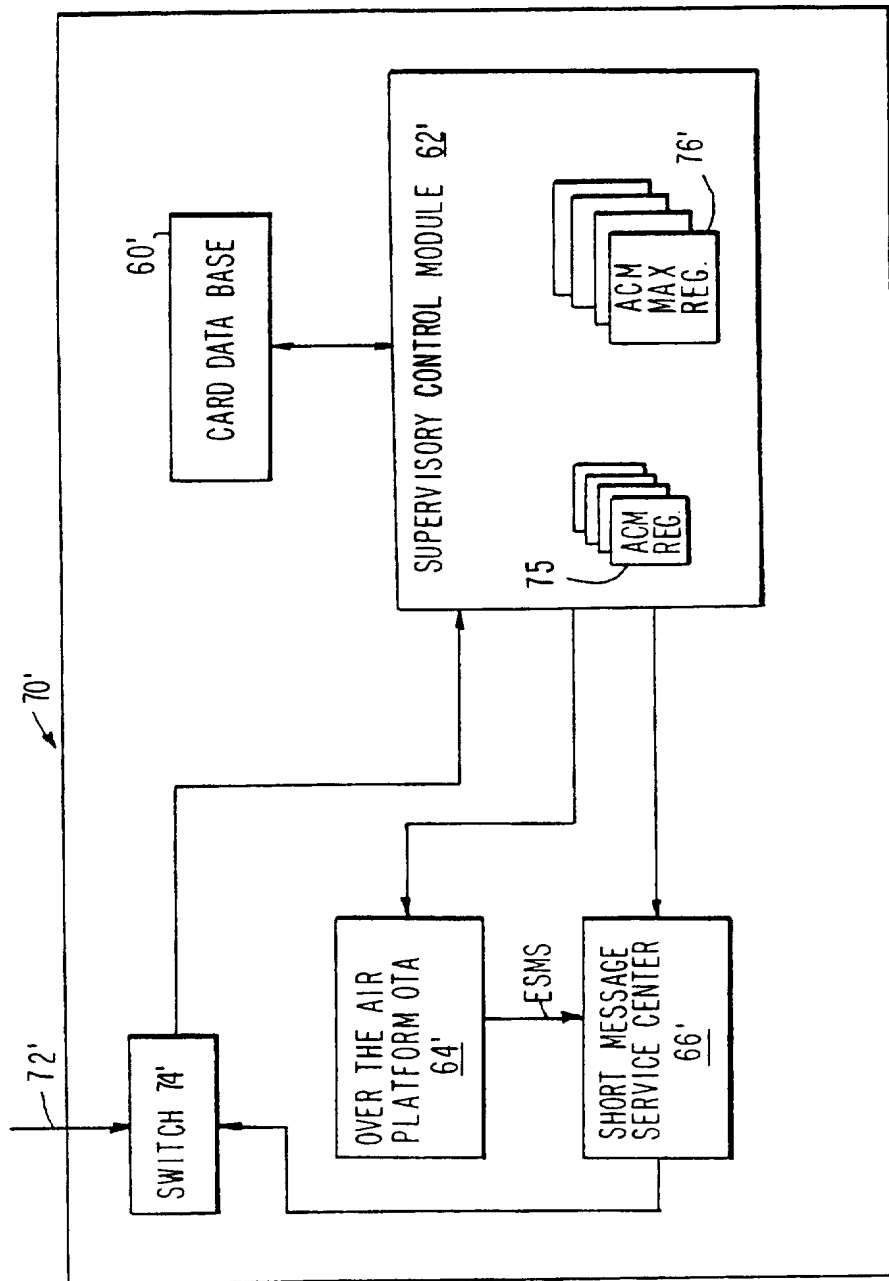
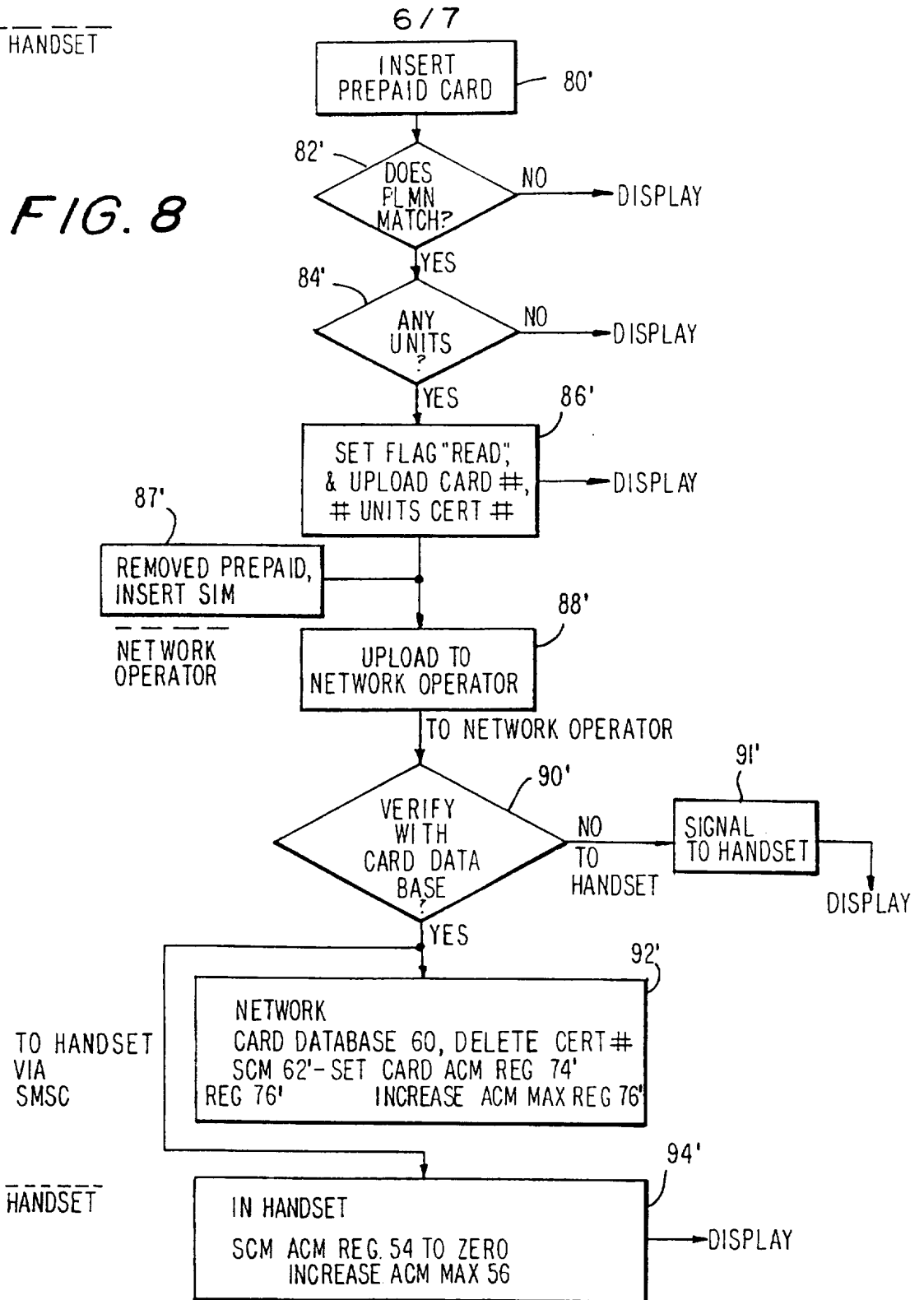


FIG. 7

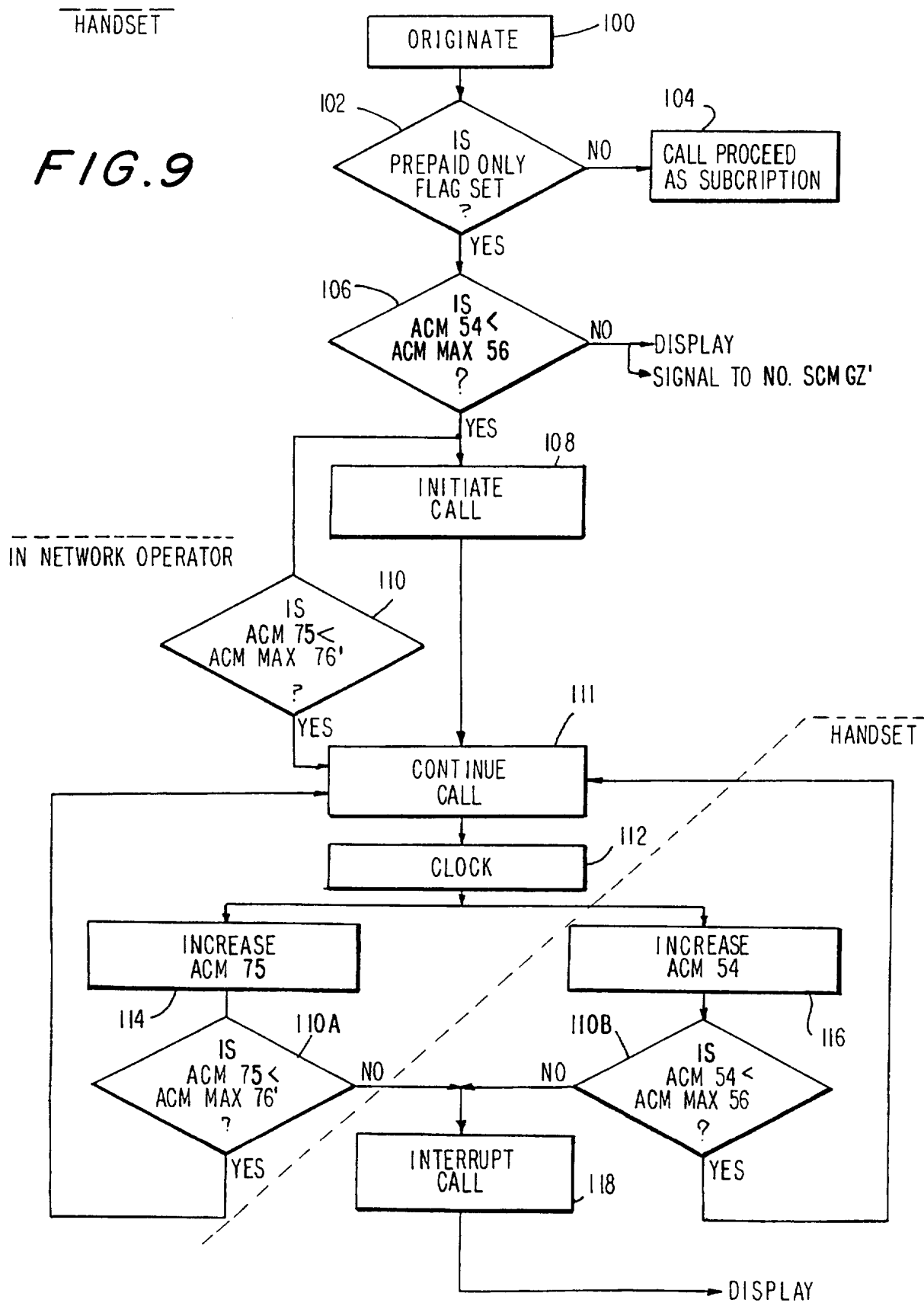
HANDSET

FIG. 8



7 / 7

FIG. 9



INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 97/00534

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M17/00 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 95 28062 A (NOKIA TELECOMMUNICATIONS OY) 19 October 1995 see the whole document ---	1-45
A	US 5 436 971 A (ARMBRUST ET AL.) 25 July 1995 see the whole document ---	1-45
A	GB 2 269 512 A (NOKIA MOBILE PHONES LIMITED) 9 February 1994 see abstract ---	1-45
P,A	WO 97 05729 A (TELECOM ITALIA MOBILE S.P.A.) 13 February 1997 see the whole document -----	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

4 August 1997

Date of mailing of the international search report

14.08.97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+ 31-70) 340-3016

Authorized officer

Montalbano, F

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 97/00534

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9528062 A	19-10-95	AU 2216795 A EP 0754394 A FI 963996 A	30-10-95 22-01-97 05-12-96
US 5436971 A	25-07-95	DE 4219739 A EP 0574990 A JP 6215208 A	23-12-93 22-12-93 05-08-94
GB 2269512 A	09-02-94	AU 4435393 A CN 1086367 A DE 586081 T EP 0586081 A JP 7312630 A	10-02-94 04-05-94 15-05-97 09-03-94 28-11-95
WO 9705729 A	13-02-97	IT RM950521 A AU 6667896 A	27-01-97 26-02-97